ID: 323078
Sample Name: ORDER PMX-PT-2001 STOCK+NOVO.exe
Cookbook: default.jbs
Time: 09:53:28
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

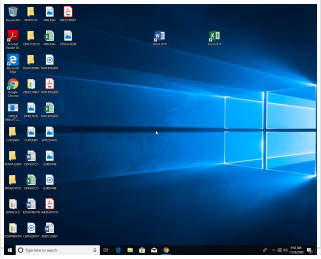
Analysis Report ORDER PMX-PT-2001 STOCK+NOVO.exe

Overview

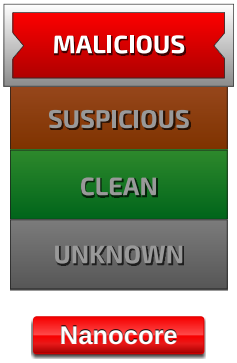
General Information

Sample Name:	ORDER PMX-PT-2001 STOCK+NOVO.exe
Analysis ID:	323078
MD5:	ce724d85d46154..
SHA1:	5de819c63b446c..
SHA256:	7534a4ffb8ef831...
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection

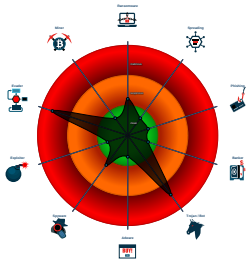


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- ORDER PMX-PT-2001 STOCK+NOVO.exe (PID: 7136 cmdline: 'C:\Users\user\Desktop\ORDER PMX-PT-2001 STOCK+NOVO.exe' MD5: CE724D85D4615439FF27F5573C9AAA8F)
  - schtasks.exe (PID: 5776 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\OBtaLehuZHtd' /XML 'C:\Users\user\AppData\Local\Temp\tmp1BEF.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5780 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 4544 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe MD5: 88BBB7610152B48C2B3879473B17857E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.592799411.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000003.00000002.592799411.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.592799411.000000000040 2000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000000.00000002.360073804.0000000003FD D000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1109d:$x1: NanoCore.ClientPluginHost • 0x438bd:$x1: NanoCore.ClientPluginHost • 0x110da:$x2: IClientNetworkHost • 0x438fa:$x2: IClientNetworkHost • 0x14c0d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x4742d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.360073804.0000000003FD D000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.MSBuild.exe.5960000.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
3.2.MSBuild.exe.5960000.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
3.2.MSBuild.exe.5960000.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
3.2.MSBuild.exe.54f0000.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
3.2.MSBuild.exe.54f0000.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 7 entries				

Sigma Overview

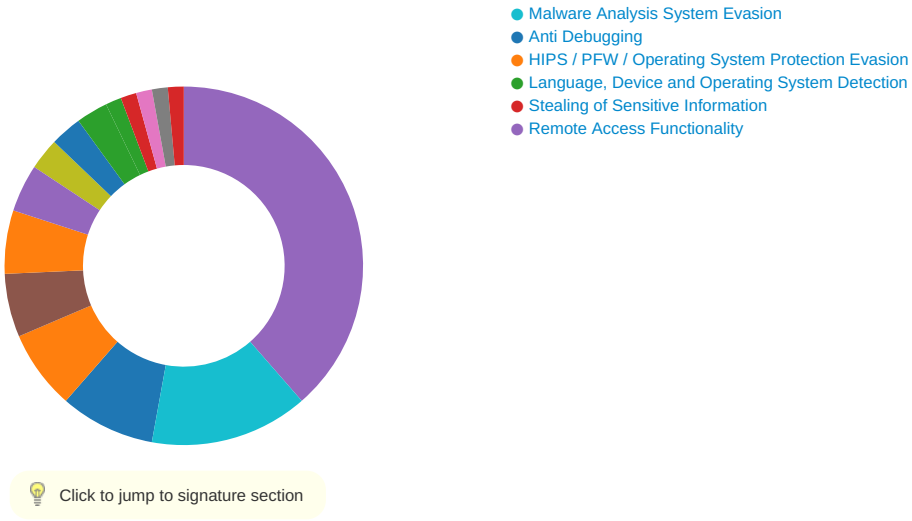
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview

- AV Detection
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection



Click to jump to signature section

AV Detection:

- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation:

- .NET source code contains potential unpacker

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)

Malware Analysis System Evasion:

- Yara detected AntiVM_3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

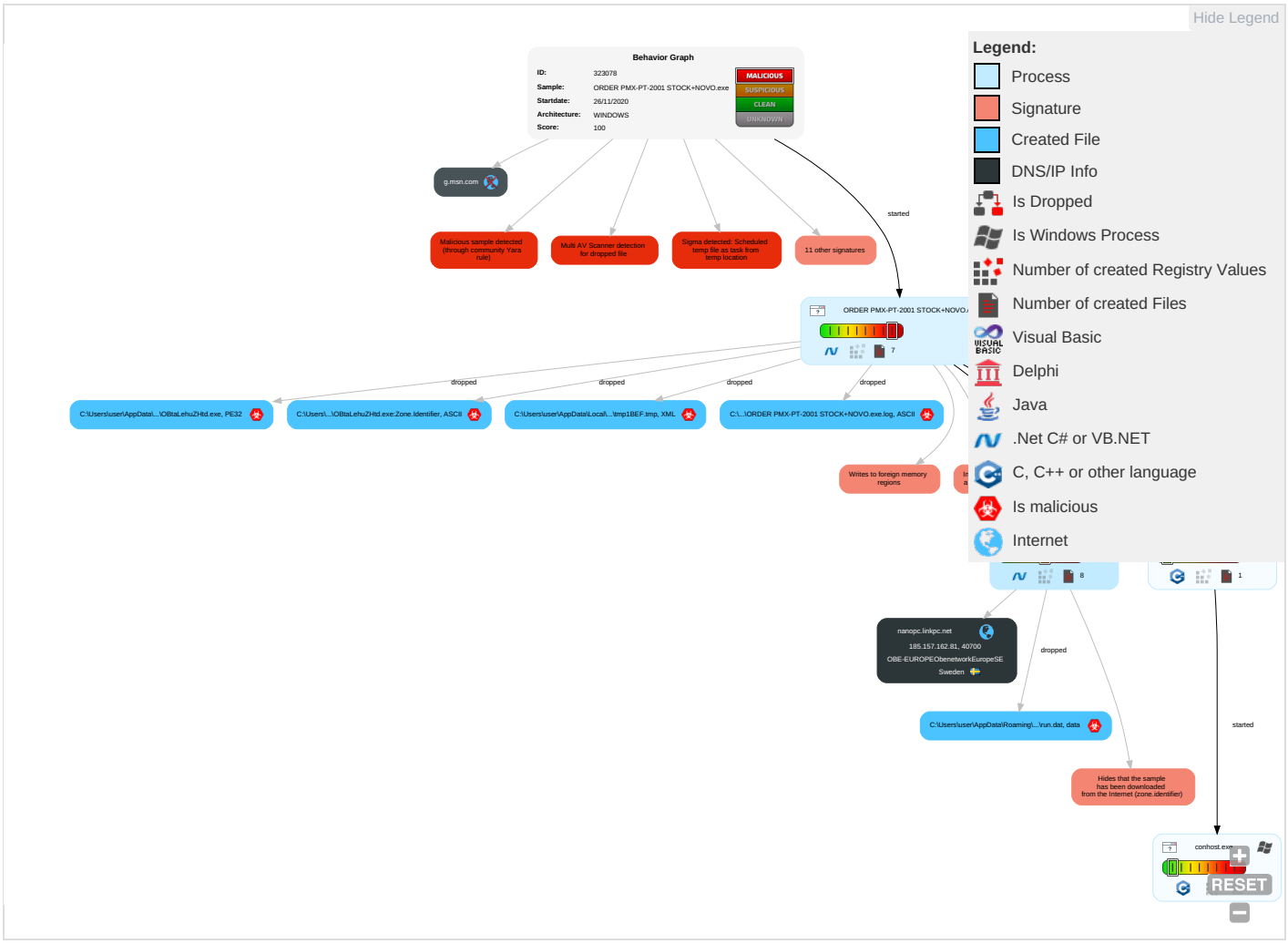
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 1	Input Capture 1 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 2 1 2	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
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	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 2 1 2	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 2	Proc Filesystem	System Information Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

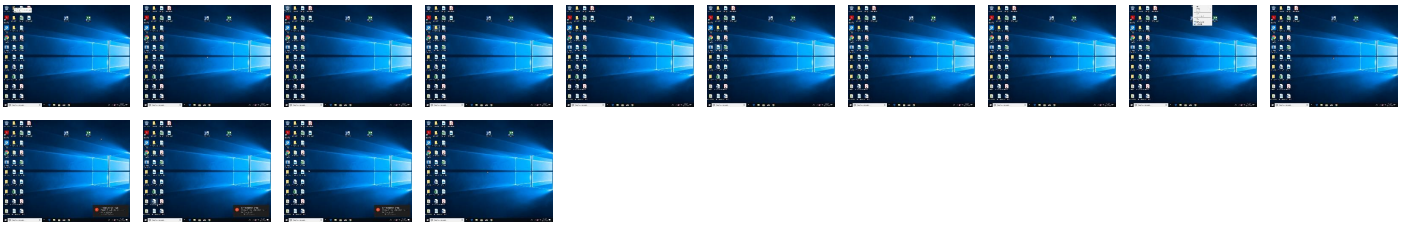
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ORDER PMX-PT-2001 STOCK+NOVO.exe	30%	Virustotal		Browse
ORDER PMX-PT-2001 STOCK+NOVO.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\OBtaLehuZHtd.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\OBtaLehuZHtd.exe	30%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.MSBuild.exe.5960000.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File
3.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

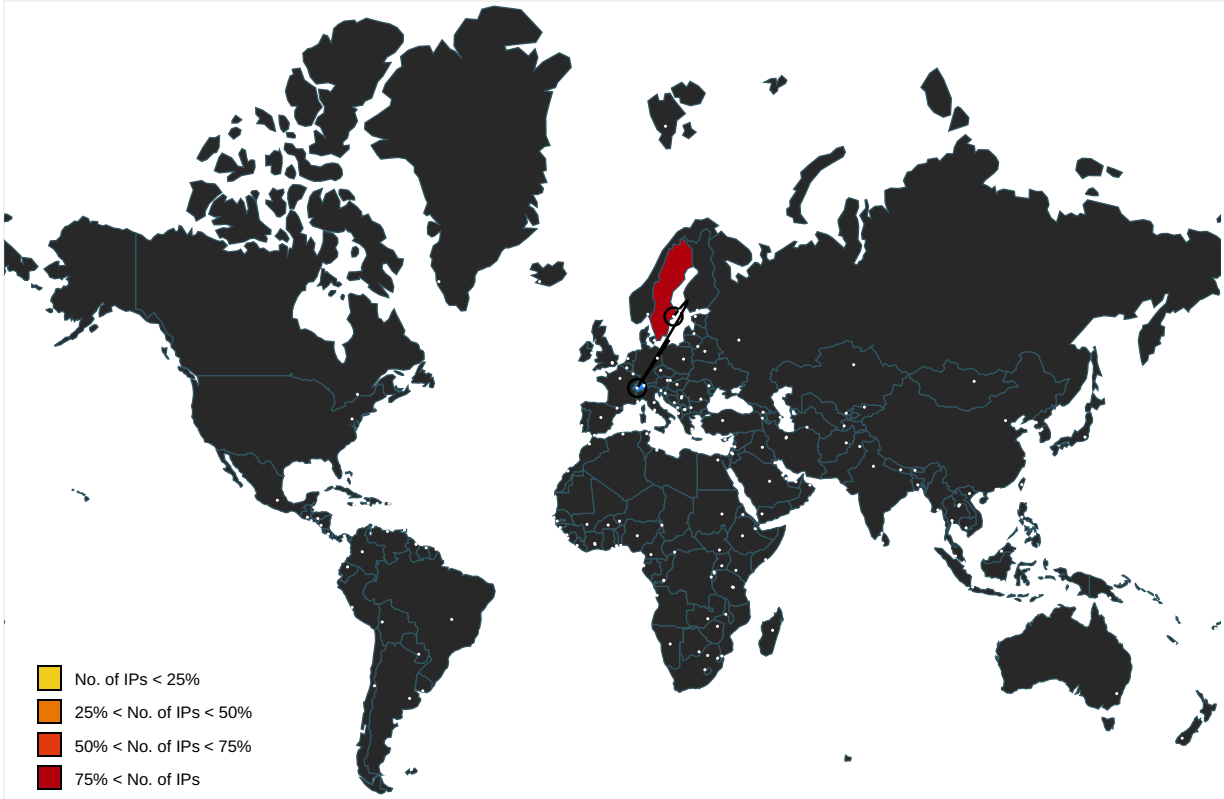
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nanopc.linkpc.net	185.157.162.81	true	false		high
g.msn.com	unknown	unknown	false		high

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323078
Start date:	26.11.2020
Start time:	09:53:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ORDER PMX-PT-2001 STOCK+NOVO.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:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/5@4/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.7% (good quality ratio 1.9%) • Quality average: 41.7% • Quality standard deviation: 33.4%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 51.104.139.180, 40.88.32.150, 52.155.217.156, 20.54.26.129, 67.27.235.126, 67.27.233.254, 8.253.95.120, 8.248.119.254, 8.253.95.249, 8.248.117.254, 67.27.234.126, 67.27.233.126, 51.103.5.186, 92.122.213.194, 92.122.213.247, 52.142.114.176, 13.64.90.137, 23.210.248.85, 104.42.151.234 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:54:28	API Interceptor	1x Sleep call for process: ORDER PMX-PT-2001 STOCK+NOVO.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.157.162.81	DHL_10177_R293_DOCUMENT.exe	Get hash	malicious	Browse	
	Order_List_PO# 081928.pdf.exe	Get hash	malicious	Browse	
	CF09550WJ901.pdf.exe	Get hash	malicious	Browse	
	Order List PO# 081927.pdf.exe	Get hash	malicious	Browse	
	Doc#66202009475352576530149 9.pdf.exe	Get hash	malicious	Browse	
	Doc#6620200947535257653014.pdf.exe	Get hash	malicious	Browse	
	Doc#6620200947535257653014 1.pdf.exe	Get hash	malicious	Browse	
	Doc#6620200947535257650358 8.pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
nanopc.linkpc.net	DHL_10177_R293_DOCUMENT.exe	Get hash	malicious	Browse	• 105.112.101.201

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OBE-EUROPEObenetworkEuropeSE	Ubnccbruoun7.exe	Get hash	malicious	Browse	• 185.157.160.228
	DHL_10177_R293_DOCUMENT.exe	Get hash	malicious	Browse	• 185.157.162.81
	INQUIRY ORDER.doc	Get hash	malicious	Browse	• 194.32.146.99
	INQUIRY ORDER.doc	Get hash	malicious	Browse	• 194.32.146.99
	INQUIRY ORDER.doc	Get hash	malicious	Browse	• 194.32.146.99
	http://https://cdn-34.anonfiles.com/J57b98L9o5/7860f6e3-1602497583/%D8%AA%D8%B7%D8%A8%D9%8A%D9%82%20%D8%A7%D9%84%D9%87%D8%AC%D8%A7%D8%A1%20%D9%84%D9%87%D8%A7%D8%AA%D9%81%20%D8%A7%D9%84%D8%A7%D9%94%D9%86%D8%AF%D8%B1%D9%88%D9%8A%D8%AF.apk	Get hash	malicious	Browse	• 45.148.16.57
	Estado_de_Cargamentos_811012912_Impo_2020-10-05_28.exe	Get hash	malicious	Browse	• 45.148.16.42
	Order_List_PO# 081928.pdf.exe	Get hash	malicious	Browse	• 185.157.162.81
	SecuriteInfo.com.Variant.Bulz.82555.20565.exe	Get hash	malicious	Browse	• 45.148.16.42
	StormKitty-1.exe	Get hash	malicious	Browse	• 45.148.16.42
	CF09550WJ901.pdf.exe	Get hash	malicious	Browse	• 185.157.162.81
	Order List PO# 081927.pdf.exe	Get hash	malicious	Browse	• 185.157.162.81
	SJNRsFNyLl.exe	Get hash	malicious	Browse	• 185.86.106.226
	5MkE8H6Sj3.exe	Get hash	malicious	Browse	• 185.86.106.226
	Doc#66202009475352576530149 9.pdf.exe	Get hash	malicious	Browse	• 185.157.162.81
	Doc#6620200947535257653014.pdf.exe	Get hash	malicious	Browse	• 185.157.162.81
	Doc#6620200947535257653014 1.pdf.exe	Get hash	malicious	Browse	• 185.157.162.81
	Doc#6620200947535257650358 8.pdf.exe	Get hash	malicious	Browse	• 185.157.162.81

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\ORDER PMX-PT-2001 STOCK+NOVO.exe.log	
Process:	C:\Users\user\Desktop\ORDER PMX-PT-2001 STOCK+NOVO.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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**
Reputation:	moderate, very likely benign file
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\Temp\tmp1BEF.tmp	
Process:	C:\Users\user\Desktop\ORDER PMX-PT-2001 STOCK+NOVO.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1657
Entropy (8bit):	5.157751041368054
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3bNtn:cbha7JlNQV/rydbz9l3YODOLNdq3Nn
MD5:	74821BCF48A29DFDAC349F3B5F24FBA6
SHA1:	3F53F7A7216A6F7A19925A1E32ACFF93524BB193
SHA-256:	AB72A4ACD0BE4653293D77A1614FBC63109353265FB80C5B10A44CE869BFFBCD
SHA-512:	77E5A7B48AD83C4211E99D5F5C728FF5342A28433C3D95E3FF93E1B0678D4DDF089B69EAE3D2C54E9F4E35479FA4513080F2760B342417F41A275FE293D0049C
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>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

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:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:RJ:RJ
MD5:	C20A2B30ACBEAD57F5255DC21D03E9C0
SHA1:	2988004D70BE62B288FAB10D0432A32A0CF68DB9
SHA-256:	EF193A49FF3C77515747A1701E68137B4DBE6DD696842DC5FD9B646EF6C221B5
SHA-512:	FF39C1A1BBE1C1495D1AC247F50597DD337882F143709700D07F656B4D0BF4816C7E5BF7BDD61E405CBBD449C1A7D1354AD9EB7C618CF5594038CEA0FA3D5DE
Malicious:	**true**
Preview:	...S4..H

C:\Users\user\AppData\Roaming\OBtaLehuZHtd.exe	
Process:	C:\Users\user\Desktop\ORDER PMX-PT-2001 STOCK+NOVO.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\user\AppData\Roaming\OBtaLehuZHtd.exe	
Category:	dropped
Size (bytes):	927232
Entropy (8bit):	7.256115423544032
Encrypted:	false
SSDEEP:	12288:dksfO0jHdT5zPvEfeVJQ34PjKYrFTm+UVYFXXrFX9rhhq3UwZtMsf05VMrWbugS8:ioZHR5LvE2VJQUj7ElUFXa
MD5:	CE724D85D4615439FF27F5573C9AAA8F
SHA1:	5DE819C63B446CF675C69376C9D7EC478DEA9060
SHA-256:	7534A4FFB8EF83103485BCCE9D51B2AF93730A9D578E2B8B5F7FF473C0F8092D
SHA-512:	A1E21BF82145E1B7FE8B50FF63A281D571ED745035BF1CA045F9540A60A69D6638E3CC65553A33828261F0877A85CDFEFA9BFD9A9880A63EFAA2684FAC5AA95D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 30%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...7..._.....P.....8... ...@....@.. ....@.....8..S....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....$.....@..B.....8.....H.....1....d...R.....0.....(....*...0..3.....r...p. ..& ...+a%..^E.....c...5.....8.....(....(....r... p(....-. .v4?%+. .m..%&. ...Za+..r...p(....(....,. Bv.m%+. -.]R%&. }.J.Za8n...(.....-. sQ4"%+. .=.$%&8Q....r9..p(....(....-. \.}.%+. 0F..%&. .)..Za8#....(.... .#.E8....rM..p(..... a;.rZ ... a8.....s....(....%.(.....(....*..0.....('...*..0..2.....u..... ..-. ....a%...^E....!...

C:\Users\user\AppData\Roaming\OBtaLehuZHtd.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\ORDER PMX-PT-2001 STOCK+NOVO.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.256115423544032
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	ORDER PMX-PT-2001 STOCK+NOVO.exe
File size:	927232
MD5:	ce724d85d4615439ff27f5573c9aaa8f
SHA1:	5de819c63b446cf675c69376c9d7ec478dea9060
SHA256:	7534a4ffb8ef83103485bcce9d51b2af93730a9d578e2b8b5f7ff473c0f8092d
SHA512:	a1e21bf82145e1b7fe8b50ff63a281d571ed745035bf1ca045f9540a60a69d6638e3cc65553a33828261f0877a85cdfefa9bfd9a9880a63efaa2684fac5aa95d
SSDEEP:	12288:dksfO0jHdT5zPvEfeVJQ34PjKYrFTm+UVYFXXrFX9rhhq3UwZtMsf05VMrWbugS8:ioZHR5LvE2VJQUj7ElUFXa
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...7..._.....P.....8... ...@....@.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4e38fe
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:	0x5FBF0837 [Thu Nov 26 01:43:19 2020 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

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe38a8	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe4000	0x610	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xe1904	0xe1a00	False	0.676799471953	data	7.26187672346	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe4000	0x610	0x800	False	0.33154296875	data	3.44562136373	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe6000	0xc	0x200	False	0.041015625	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe40a0	0x380	data		
RT_MANIFEST	0xe4420	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

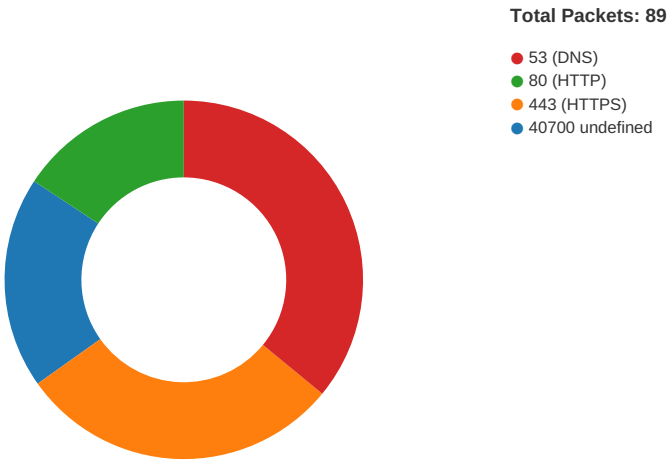
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Hewlett-Packard 2017
Assembly Version	1.0.0.0
InternalName	2e6s.exe
FileVersion	1.0.0.0
CompanyName	Hewlett-Packard
LegalTrademarks	
Comments	
ProductName	Arizona Lottery Numbers
ProductVersion	1.0.0.0
FileDescription	Arizona Lottery Numbers
OriginalFilename	2e6s.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 09:54:33.876842022 CET	49714	40700	192.168.2.6	185.157.162.81
Nov 26, 2020 09:54:36.877525091 CET	49714	40700	192.168.2.6	185.157.162.81
Nov 26, 2020 09:54:42.416287899 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:54:42.416327000 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:54:42.416387081 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:54:42.416420937 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:54:42.586405039 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.586430073 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.586441040 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.586456060 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.586472034 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.586487055 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.586503983 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.586524010 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.586540937 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.586555958 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:54:42.586587906 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:54:42.586608887 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.586667061 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:54:42.598721027 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.598757029 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.598786116 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.598810911 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:54:42.598826885 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.598855019 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.598875046 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:54:42.598884106 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.598921061 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.598936081 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:54:42.598953962 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.599004984 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.599005938 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:54:42.599044085 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.599104881 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:54:42.612081051 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.612124920 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.612160921 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.612184048 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:54:42.612198114 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.612236977 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.612262011 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:54:42.612273932 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.612313032 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.612333059 CET	49678	443	192.168.2.6	40.90.22.191

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 09:54:42.612353086 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.612402916 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.612410069 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:54:42.612441063 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:54:42.612504005 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:54:42.877913952 CET	49714	40700	192.168.2.6	185.157.162.81
Nov 26, 2020 09:54:52.692703009 CET	49720	40700	192.168.2.6	185.157.162.81
Nov 26, 2020 09:54:55.740345955 CET	49720	40700	192.168.2.6	185.157.162.81
Nov 26, 2020 09:55:01.739180088 CET	49720	40700	192.168.2.6	185.157.162.81
Nov 26, 2020 09:55:03.849091053 CET	49682	80	192.168.2.6	2.20.142.210
Nov 26, 2020 09:55:03.849329948 CET	49684	80	192.168.2.6	93.184.220.29
Nov 26, 2020 09:55:03.865498066 CET	80	49682	2.20.142.210	192.168.2.6
Nov 26, 2020 09:55:03.865514994 CET	80	49684	93.184.220.29	192.168.2.6
Nov 26, 2020 09:55:03.865608931 CET	49682	80	192.168.2.6	2.20.142.210
Nov 26, 2020 09:55:03.865685940 CET	49684	80	192.168.2.6	93.184.220.29
Nov 26, 2020 09:55:04.052180052 CET	80	49681	93.184.220.29	192.168.2.6
Nov 26, 2020 09:55:04.052809000 CET	49681	80	192.168.2.6	93.184.220.29
Nov 26, 2020 09:55:04.489773035 CET	49686	443	192.168.2.6	104.108.60.202
Nov 26, 2020 09:55:04.506099939 CET	443	49686	104.108.60.202	192.168.2.6
Nov 26, 2020 09:55:04.506124973 CET	443	49686	104.108.60.202	192.168.2.6
Nov 26, 2020 09:55:04.506222010 CET	49686	443	192.168.2.6	104.108.60.202
Nov 26, 2020 09:55:04.506242037 CET	49686	443	192.168.2.6	104.108.60.202
Nov 26, 2020 09:55:04.627742052 CET	80	49685	93.184.220.29	192.168.2.6
Nov 26, 2020 09:55:04.627842903 CET	49685	80	192.168.2.6	93.184.220.29
Nov 26, 2020 09:55:05.065186977 CET	80	49680	93.184.220.29	192.168.2.6
Nov 26, 2020 09:55:05.065326929 CET	49680	80	192.168.2.6	93.184.220.29
Nov 26, 2020 09:55:05.962677002 CET	49699	443	192.168.2.6	204.79.197.200
Nov 26, 2020 09:55:07.156651020 CET	80	49702	93.184.220.29	192.168.2.6
Nov 26, 2020 09:55:07.156977892 CET	49702	80	192.168.2.6	93.184.220.29
Nov 26, 2020 09:55:08.013235092 CET	49701	443	192.168.2.6	23.210.249.50
Nov 26, 2020 09:55:08.013411999 CET	49702	80	192.168.2.6	93.184.220.29
Nov 26, 2020 09:55:11.772195101 CET	49741	40700	192.168.2.6	185.157.162.81
Nov 26, 2020 09:55:14.771539927 CET	49741	40700	192.168.2.6	185.157.162.81
Nov 26, 2020 09:55:20.787298918 CET	49741	40700	192.168.2.6	185.157.162.81
Nov 26, 2020 09:55:29.516587973 CET	49744	40700	192.168.2.6	185.157.162.81
Nov 26, 2020 09:55:32.522639990 CET	49744	40700	192.168.2.6	185.157.162.81
Nov 26, 2020 09:55:38.523539066 CET	49744	40700	192.168.2.6	185.157.162.81
Nov 26, 2020 09:55:46.481851101 CET	49747	40700	192.168.2.6	185.157.162.81
Nov 26, 2020 09:55:49.492790937 CET	49747	40700	192.168.2.6	185.157.162.81
Nov 26, 2020 09:55:52.978184938 CET	49680	80	192.168.2.6	93.184.220.29
Nov 26, 2020 09:55:52.978399038 CET	49681	80	192.168.2.6	93.184.220.29
Nov 26, 2020 09:55:52.978409052 CET	49677	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:55:52.994458914 CET	80	49680	93.184.220.29	192.168.2.6
Nov 26, 2020 09:55:52.994496107 CET	80	49681	93.184.220.29	192.168.2.6
Nov 26, 2020 09:55:52.995488882 CET	49680	80	192.168.2.6	93.184.220.29
Nov 26, 2020 09:55:52.995496988 CET	49681	80	192.168.2.6	93.184.220.29
Nov 26, 2020 09:55:53.148066044 CET	443	49677	40.90.22.191	192.168.2.6
Nov 26, 2020 09:55:53.148196936 CET	49677	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:55:53.212937117 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:55:53.382978916 CET	443	49678	40.90.22.191	192.168.2.6
Nov 26, 2020 09:55:53.383265972 CET	49678	443	192.168.2.6	40.90.22.191
Nov 26, 2020 09:55:55.493424892 CET	49747	40700	192.168.2.6	185.157.162.81
Nov 26, 2020 09:56:05.356472015 CET	49751	40700	192.168.2.6	185.157.162.81
Nov 26, 2020 09:56:06.067751884 CET	80	49685	93.184.220.29	192.168.2.6
Nov 26, 2020 09:56:06.068116903 CET	49685	80	192.168.2.6	93.184.220.29
Nov 26, 2020 09:56:08.348980904 CET	49751	40700	192.168.2.6	185.157.162.81

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 09:54:24.288594961 CET	56023	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:54:24.315777063 CET	53	56023	8.8.8.8	192.168.2.6
Nov 26, 2020 09:54:27.965220928 CET	58384	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:54:27.992178917 CET	53	58384	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 09:54:42.825367928 CET	60261	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:54:42.852485895 CET	53	60261	8.8.8.8	192.168.2.6
Nov 26, 2020 09:54:45.245971918 CET	56061	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:54:45.273152113 CET	53	56061	8.8.8.8	192.168.2.6
Nov 26, 2020 09:54:46.775904894 CET	58336	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:54:46.802928925 CET	53	58336	8.8.8.8	192.168.2.6
Nov 26, 2020 09:54:47.892515898 CET	53781	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:54:47.919559002 CET	53	53781	8.8.8.8	192.168.2.6
Nov 26, 2020 09:54:58.179836988 CET	54064	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:54:58.207010031 CET	53	54064	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:00.410944939 CET	52811	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:00.446618080 CET	53	52811	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:01.018721104 CET	55299	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:01.054347992 CET	53	55299	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:01.467667103 CET	63745	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:01.505188942 CET	53	63745	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:01.791971922 CET	50055	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:01.827680111 CET	53	50055	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:02.158008099 CET	61374	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:02.176760912 CET	50339	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:02.193687916 CET	53	61374	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:02.203960896 CET	53	50339	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:03.128297091 CET	63307	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:03.163994074 CET	53	63307	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:03.682431936 CET	49694	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:03.718391895 CET	53	49694	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:03.918296099 CET	54982	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:03.945344925 CET	53	54982	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:04.000586987 CET	50010	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:04.027589083 CET	53	50010	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:04.279766083 CET	63718	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:04.306961060 CET	53	63718	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:05.008614063 CET	62116	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:05.044142008 CET	53	62116	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:05.400423050 CET	63816	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:05.427606106 CET	53	63816	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:05.814524889 CET	55014	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:05.850156069 CET	53	55014	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:11.313044071 CET	62208	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:11.352133036 CET	53	62208	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:14.762459993 CET	57574	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:14.805686951 CET	53	57574	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:28.665090084 CET	51818	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:28.692254066 CET	53	51818	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:29.373004913 CET	56628	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:29.514488935 CET	53	56628	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:29.837275028 CET	60778	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:29.864356995 CET	53	60778	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:39.535485029 CET	53799	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:39.562618017 CET	53	53799	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:46.442470074 CET	54683	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:46.480175018 CET	53	54683	8.8.8.8	192.168.2.6
Nov 26, 2020 09:55:49.509167910 CET	59329	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:55:49.548579931 CET	53	59329	8.8.8.8	192.168.2.6
Nov 26, 2020 09:56:05.202418089 CET	64021	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:56:05.355149031 CET	53	64021	8.8.8.8	192.168.2.6
Nov 26, 2020 09:56:06.826370001 CET	56129	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:56:06.853466988 CET	53	56129	8.8.8.8	192.168.2.6
Nov 26, 2020 09:56:12.634813070 CET	58177	53	192.168.2.6	8.8.8.8
Nov 26, 2020 09:56:12.661889076 CET	53	58177	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 09:55:14.762459993 CET	192.168.2.6	8.8.8.8	0x4d36	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 26, 2020 09:55:29.373004913 CET	192.168.2.6	8.8.8.8	0x827e	Standard query (0)	nanopc.linkpc.net	A (IP address)	IN (0x0001)
Nov 26, 2020 09:55:46.442470074 CET	192.168.2.6	8.8.8.8	0x313a	Standard query (0)	nanopc.linkpc.net	A (IP address)	IN (0x0001)
Nov 26, 2020 09:56:05.202418089 CET	192.168.2.6	8.8.8.8	0xc233	Standard query (0)	nanopc.linkpc.net	A (IP address)	IN (0x0001)

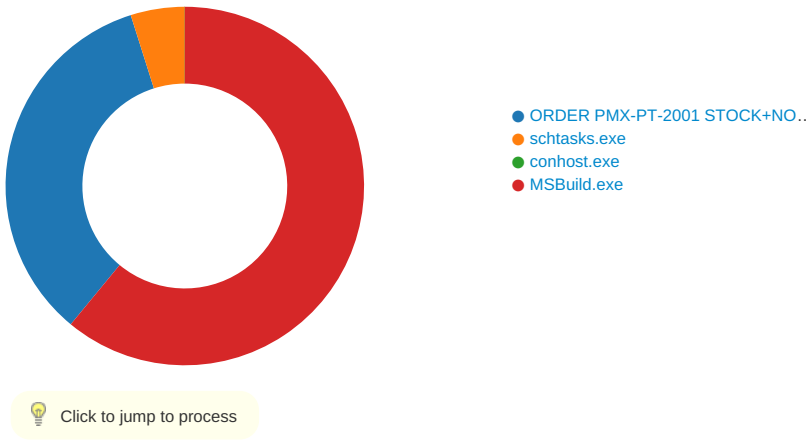
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 09:55:14.805686951 CET	8.8.8.8	192.168.2.6	0x4d36	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 09:55:29.514488935 CET	8.8.8.8	192.168.2.6	0x827e	No error (0)	nanopc.linkpc.net		185.157.162.81	A (IP address)	IN (0x0001)
Nov 26, 2020 09:55:46.480175018 CET	8.8.8.8	192.168.2.6	0x313a	No error (0)	nanopc.linkpc.net		185.157.162.81	A (IP address)	IN (0x0001)
Nov 26, 2020 09:56:05.355149031 CET	8.8.8.8	192.168.2.6	0xc233	No error (0)	nanopc.linkpc.net		185.157.162.81	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: ORDER PMX-PT-2001 STOCK+NOVO.exe PID: 7136 Parent PID: 5832

General

Start time:	09:54:18
Start date:	26/11/2020

Path:	C:\Users\user\Desktop\ORDER PMX-PT-2001 STOCK+NOVO.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ORDER PMX-PT-2001 STOCK+NOVO.exe'
Imagebase:	0x690000
File size:	927232 bytes
MD5 hash:	CE724D85D4615439FF27F5573C9AAA8F
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: 00000000.00000002.360073804.0000000003FDD000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.360073804.0000000003FDD000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.360073804.0000000003FDD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.357258593.0000000002F01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.357341507.0000000002F8C000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Roaming\OBtaLehuZHtd.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	54B06FC	CopyFileW
C:\Users\user\AppData\Roaming\OBtaLehuZHtd.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	54B06FC	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp1BEF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	54B0F40	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\ORDER PMX-PT-2001 STOCK+NOVO.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1BEF.tmp	success or wait	1	54B1512	DeleteFileW

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\Roaming\OBtaLehuZHtd.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 37 08 bf 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 1a 0e 00 00 0a 00 00 00 00 00 00 fe 38 0e 00 00 20 00 00 00 40 0e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 0e 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...7.._.......... ....P.............8... ...@....@.. ....@................	success or wait	4	54B06FC	CopyFileW
C:\Users\user\AppData\Roaming\ OBtaLehuZHtd.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	54B06FC	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp1BEF.tmp	unknown	1657	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10- 25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </Registratio	success or wait	1	54B11CF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\ORDER PMX-PT-2001 STOCK+NOVO.exe.log	unknown	664	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	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.n	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: schtasks.exe PID: 5776 Parent PID: 7136

General

Start time:	09:54:29
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\OBtaLehuZHtd' /XML 'C:\Users\user\AppData\Local\Temp\tmp1BEF.tmp'
Imagebase:	0xaf0000
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\tmp1BEF.tmp	unknown	2	success or wait	1	AFAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1BEF.tmp	unknown	1658	success or wait	1	AFABD9	ReadFile

Analysis Process: conhost.exe PID: 5780 Parent PID: 5776

General

Start time:	09:54:30
Start date:	26/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: MSBuild.exe PID: 4544 Parent PID: 7136

General

Start time:	09:54:30
Start date:	26/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Imagebase:	0xba0000
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: 00000003.00000002.592799411.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.592799411.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.592799411.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.599041317.0000000005960000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.599041317.0000000005960000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.599041317.0000000005960000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.598672636.00000000054F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.598672636.00000000054F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.597422084.00000000041A7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.597422084.00000000041A7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	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	72FB60AC	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	54C07A1	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	54C089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	54C07A1	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	54C07A1	CreateDirectoryW
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	72FB60AC	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	72FB60AC	unknown

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	13 89 e7 53 34 92 d8 48	...S4..H	success or wait	1	54C0A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	54C0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	success or wait	1	54C0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	end of file	1	54C0A53	ReadFile

Disassembly

Code Analysis