

JoeSandbox Cloud BASIC



ID: 712188

Sample Name: confirm
order.exe

Cookbook: default.jbs

Time: 01:14:32

Date: 29/09/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report confirm order.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: NanoCore	4
Yara Signatures	5
Memory Dumps	5
Unpacked PEs	6
Sigma Signatures	6
AV Detection	6
E-Banking Fraud	6
Stealing of Sensitive Information	6
Remote Access Functionality	6
Snort Signatures	6
Joe Sandbox Signatures	7
AV Detection	7
Networking	7
E-Banking Fraud	7
System Summary	7
Data Obfuscation	7
Malware Analysis System Evasion	7
HIPS / PFW / Operating System Protection Evasion	7
Stealing of Sensitive Information	7
Remote Access Functionality	7
Mitre Att&ck Matrix	8
Behavior Graph	8
Screenshots	9
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	10
Initial Sample	10
Dropped Files	10
Unpacked PE Files	10
Domains	11
URLs	11
Domains and IPs	11
Contacted Domains	11
Contacted URLs	11
URLs from Memory and Binaries	11
World Map of Contacted IPs	12
Public IPs	12
Private	13
General Information	13
Warnings	13
Simulations	13
Behavior and APIs	13
Joe Sandbox View / Context	14
IPs	14
Domains	14
ASNs	14
JA3 Fingerprints	14
Dropped Files	14
Created / dropped Files	14
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\confirm order.exe.log	14
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	14
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5zzuybal.sto.ps1	15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dygbxst.ufu.psm1	15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_f2arnmm1.jms.psm1	16
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yxgpca1x.l0u.ps1	16
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	16
C:\Users\user\AppData\Roaming\Prqhnsx\Ugtphvhf.exe	16
C:\Users\user\AppData\Roaming\Prqhnsx\Ugtphvhf.exe:Zone.Identifier	17
Static File Info	17
General	17
File Icon	17

Static PE Info	17
General	17
Entrypoint Preview	18
Data Directories	18
Sections	18
Resources	18
Imports	19
Network Behavior	19
TCP Packets	19
Statistics	19
Behavior	19
System Behavior	20
Analysis Process: confirm order.exePID: 5552, Parent PID: 6092	20
General	20
File Activities	20
File Created	20
File Written	21
File Read	22
Registry Activities	22
Key Value Created	22
Analysis Process: powershell.exePID: 1756, Parent PID: 5552	22
General	22
File Activities	23
File Created	23
File Deleted	23
File Written	23
File Read	25
Analysis Process: conhost.exePID: 1652, Parent PID: 1756	26
General	26
Analysis Process: confirm order.exePID: 1020, Parent PID: 5552	27
General	27
File Activities	27
File Created	27
File Written	28
File Read	28
Analysis Process: Ugtphvhf.exePID: 5292, Parent PID: 3452	28
General	28
File Activities	29
File Created	29
File Read	29
Analysis Process: Ugtphvhf.exePID: 6072, Parent PID: 3452	29
General	29
File Activities	30
File Created	30
File Read	30
Analysis Process: powershell.exePID: 5344, Parent PID: 5292	30
General	30
File Activities	31
File Created	31
File Deleted	31
File Written	31
File Read	31
Analysis Process: conhost.exePID: 2384, Parent PID: 5344	32
General	32
Disassembly	32

Windows Analysis Report

confirm order.exe

Overview

General Information

Sample Name:

confirm order.exe

Analysis ID:

712188

MD5:

e5e6a926238dfe..

SHA1:

b2332282693679..

SHA256:

219eeb73337cb0..

Tags:

exe

NanoCore

RAT

Infos:

YARA SIGNA

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Nanocore

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Multi AV Scanner detection for subm...

Malicious sample detected (through...

Sigma detected: NanoCore

Detected Nanocore Rat

Antivirus detection for URL or domain

Multi AV Scanner detection for dom...

Multi AV Scanner detection for drop...

Yara detected Nanocore RAT

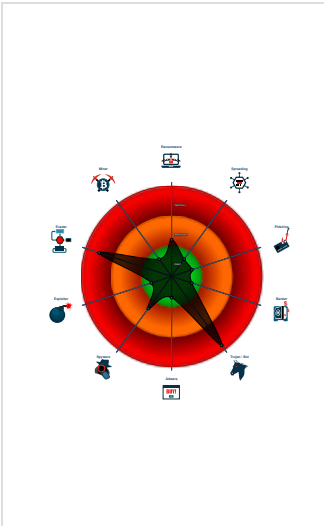
Initial sample is a PE file and has a...

Connects to many ports of the same...

Tries to detect sandboxes and other...

Yara detected Costura Assembly Lo...

Classification



Process Tree

System is w10x64

confirm order.exe

(PID: 5552 cmdline: "C:\Users\user\Desktop\confirm order.exe" MD5: E5E6A926238DFECD931967194FF92BF4)

powershell.exe

(PID: 1756 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQB TAGUAYwBvAG4AZABzACAANgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)

conhost.exe

(PID: 1652 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

confirm order.exe

(PID: 1020 cmdline: C:\Users\user\Desktop\confirm order.exe MD5: E5E6A926238DFECD931967194FF92BF4)

Ugtphvhf.exe

(PID: 5292 cmdline: "C:\Users\user\AppData\Roaming\Prqhnsx\Ugtphvhf.exe" MD5: E5E6A926238DFECD931967194FF92BF4)

powershell.exe

(PID: 5344 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQB TAGUAYwBvAG4AZABzACAANgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)

conhost.exe

(PID: 2384 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

Ugtphvhf.exe

(PID: 6072 cmdline: "C:\Users\user\AppData\Roaming\Prqhnsx\Ugtphvhf.exe" MD5: E5E6A926238DFECD931967194FF92BF4)

cleanup

Malware Configuration

Threatname: NanoCore

Copyright Joe Security LLC 2022

Page 4 of 32

```
{
  "Version": "1.2.2.0",
  "Mutex": "6a8dc68c-2ae6-4a66-b5dc-80cfa679",
  "Group": "jop",
  "Domain1": "146.70.76.43",
  "Domain2": "",
  "Port": 56281,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Disable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 9,
  "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 Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.447081649.00000000031D1000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000000.00000002.447887037.00000000032BD000.0000004.00000800.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0x3c9d9:\$x1: NanoCore.ClientPluginHost 0x3ca16:\$x2: IClientNetworkHost 0x40549:\$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.447887037.00000000032BD000.0000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0x3c741:\$a: NanoCore 0x3c751:\$a: NanoCore 0x3c985:\$a: NanoCore 0x3c999:\$a: NanoCore 0x3c9d9:\$a: NanoCore 0x3c7a0:\$b: ClientPlugin 0x3c9a2:\$b: ClientPlugin 0x3c9e2:\$b: ClientPlugin 0x3c8c7:\$c: ProjectData 0x3d2ce:\$d: DESCrypto 0x3ee83:\$i: get_Connected 0x3d604:\$j: #=q 0x3d634:\$j: #=q 0x3d650:\$j: #=q 0x3d680:\$j: #=q 0x3d69c:\$j: #=q 0x3d6b8:\$j: #=q 0x3d6e8:\$j: #=q 0x3d704:\$j: #=q 0x3d748:\$j: #=q 0x3d764:\$j: #=q
00000000.00000002.447887037.00000000032BD000.0000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	0x3c9d9:\$a1: NanoCore.ClientPluginHost 0x3c999:\$a2: NanoCore.ClientPlugin 0x3e8f2:\$b1: get_BuilderSettings 0x3c7f5:\$b2: ClientLoaderForm.resources 0x3e012:\$b3: PluginCommand 0x3c9ca:\$b4: IClientAppHost 0x3ef4a:\$b6: AddHostEntry 0x3eeb7:\$b8: PipeExists 0x3ca03:\$b9: IClientLoggingHost

Source	Rule	Description	Author	Strings
00000000.00000002.454452204.0000000004322000.0000004.00000800.00020000.00000000.sdmpr	Nanocore_RAT_Gen_2	Detetctcs the Nanocore RAT	Florian Roth	0x106ad:\$x1: NanoCore.ClientPluginHost 0x42ecd:\$x1: NanoCore.ClientPluginHost 0x106ea:\$x2: IClientNetworkHost 0x42f0a:\$x2: IClientNetworkHost 0x1421d:\$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJlLdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe 0x46a3d:\$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJlLdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 49 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.confirm order.exe.6010000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetctcs the Nanocore RAT	Florian Roth	0xf7ad:\$x1: NanoCore.ClientPluginHost 0xf7da:\$x2: IClientNetworkHost
14.2.confirm order.exe.6010000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	0xf7ad:\$x2: NanoCore.ClientPluginHost 0x10888:\$s4: PipeCreated 0xf7c7:\$s5: IClientLoggingHost
14.2.confirm order.exe.6010000.6.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
14.2.confirm order.exe.6010000.6.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	0xf778:\$x2: NanoCore.ClientPlugin 0xf7ad:\$x3: NanoCore.ClientPluginHost 0xf76c:\$i2: IClientData 0xf78e:\$i3: IClientNetwork 0xf79d:\$i5: IClientDataHost 0xf7c7:\$i6: IClientLoggingHost 0xf7da:\$i7: IClientNetworkHost 0xf7ed:\$i8: IClientUIHost 0xf7fb:\$i9: IClientNameObjectCollection 0xf817:\$i10: IClientReadOnlyNameObjectCollection 0xf56a:\$s1: ClientPlugin 0xf781:\$s1: ClientPlugin 0x147a2:\$s6: get_ClientSettings
14.2.confirm order.exe.6010000.6.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	0xf7ad:\$a1: NanoCore.ClientPluginHost 0xf778:\$a2: NanoCore.ClientPlugin 0x146f3:\$b1: get_BuilderSettings 0x14662:\$b7: LogClientException 0xf7c7:\$b9: IClientLoggingHost
Click to see the 98 entries				

Sigma Signatures

AV Detection



Sigma detected: NanoCore

E-Banking Fraud



Sigma detected: NanoCore

Stealing of Sensitive Information



Sigma detected: NanoCore

Remote Access Functionality



Sigma detected: NanoCore

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking



Connects to many ports of the same IP (likely port scanning)

C2 URLs / IPs found in malware configuration

E-Banking Fraud



Yara detected Nanocore RAT

System Summary



Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation



Yara detected Costura Assembly Loader

.NET source code contains potential unpacker

Malware Analysis System Evasion



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

HIPS / PFW / Operating System Protection Evasion



Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

Stealing of Sensitive Information



Yara detected Nanocore RAT

Remote Access Functionality



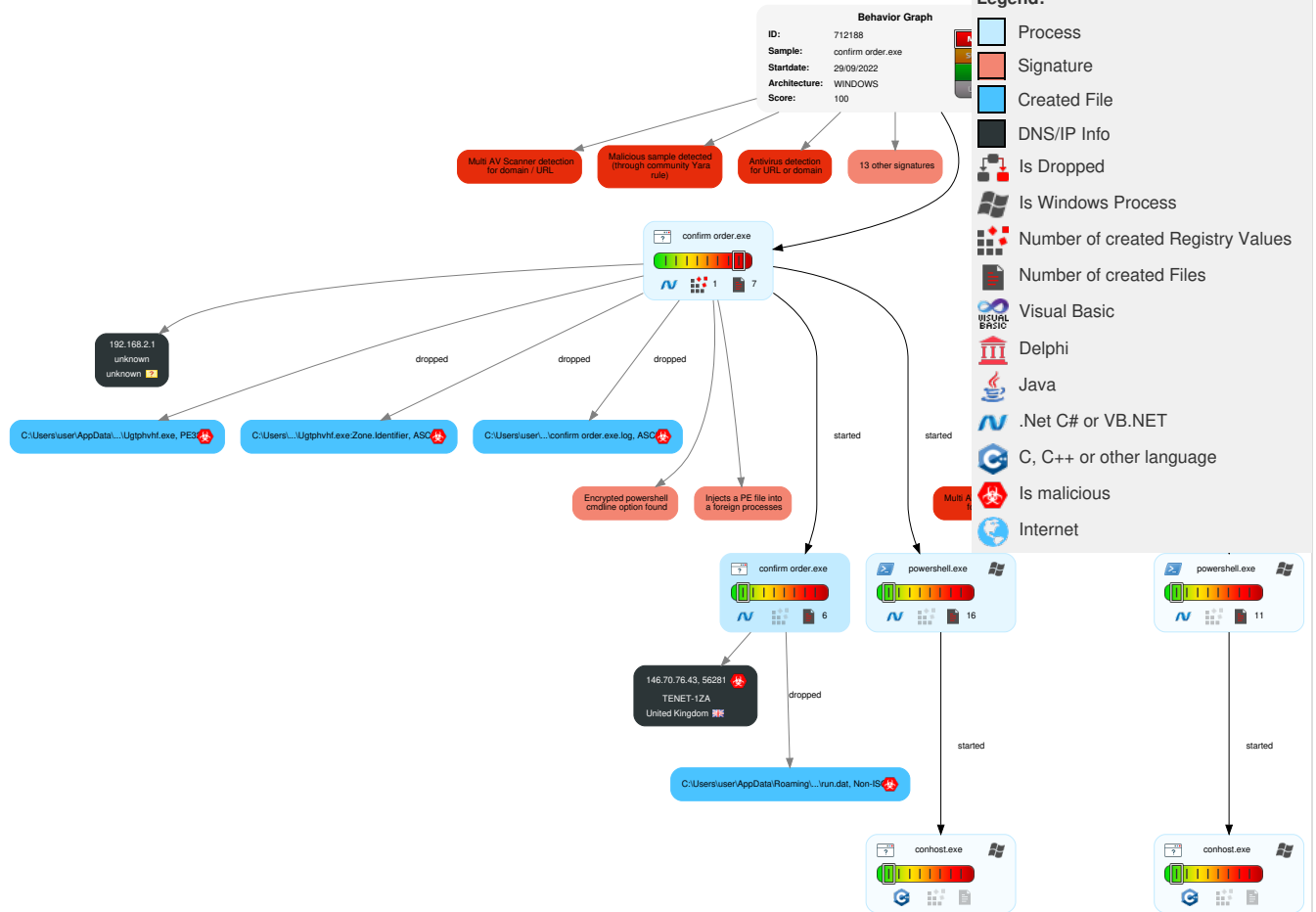
Detected Nanocore Rat

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	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 PowerShell	1 Registry Run Keys / Startup Folder	1 1 2 Process Injection	1 Masquerading	1 1 Input Capture	2 1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Deobfuscate/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Timestamp	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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
confirm order.exe	40%	ReversingLabs	ByteCode-MSIL.Trojan.Woref lint	
confirm order.exe	49%	Virustotal		Browse
confirm order.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Prqhnsx\Ugtphvhf.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Prqhnsx\Ugtphvhf.exe	40%	ReversingLabs	ByteCode-MSIL.Trojan.Woref lint	
C:\Users\user\AppData\Roaming\Prqhnsx\Ugtphvhf.exe	49%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.0.confirm order.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
14.2.confirm order.exe.6010000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.confirm order.exe.32e984c.0.unpack	100%	Avira	HEUR/AGEN.1211686		Download File

Domains

 No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
146.70.76.43	7%	Virustotal		Browse
146.70.76.43	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

 No contacted domains info

Contacted URLs

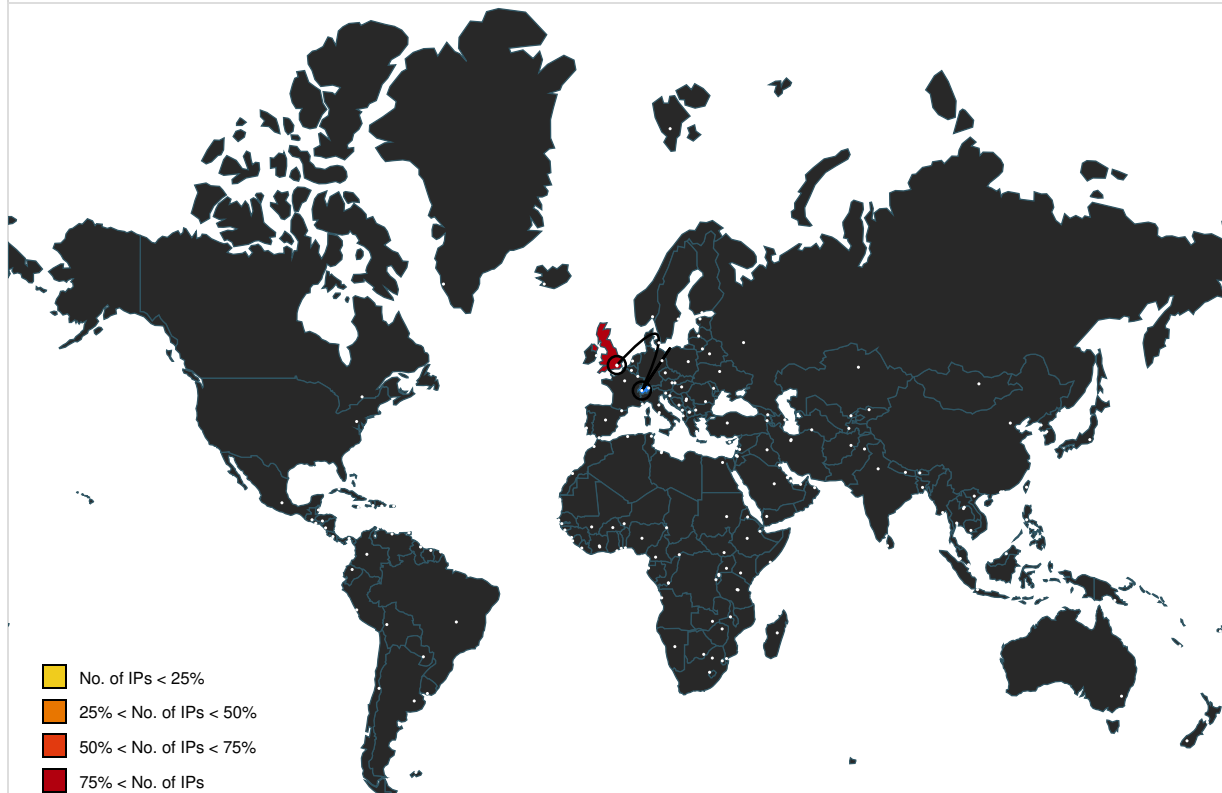
Name	Malicious	Antivirus Detection	Reputation
	true	Avira URL Cloud: safe	low
146.70.76.43	true	7%, Virustotal, Browse - Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.newtonsoft.com/json	confirm order.exe, 00000000.00000002.454452204.0000000004322000.00000004.00000800.0.00020000.00000000.sdmp, confirm order.exe, 00000000.00000002.455433787.00000000057E0000.00000004.08000000.00040000.00000000.sdmp, confirm order.exe, 00000000.00000002.452265867.0000000036D4000.00000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 0000000F.00000002.549759132.0000000002E84000.0000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 0000000F.00000002.563157770.000000003B29000.00000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 00000010.00000002.563162662.0000000004189000.0000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 00000010.00000002.549878196.00000000034E4000.00000004.00000800.0020000.00000000.sdmp, Ugtphvhf.exe, 00000010.00000002.561455007.00000000040E9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.nuget.org/packages/Newtonsoft.Json.Bson	confirm order.exe, 00000000.00000002.454452204.0000000004322000.00000004.00000800.0.00020000.00000000.sdmp, confirm order.exe, 00000000.00000002.455433787.00000000057E0000.00000004.08000000.00040000.00000000.sdmp, confirm order.exe, 00000000.00000002.452265867.0000000036D4000.00000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 0000000F.00000002.549759132.0000000002E84000.0000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 00000010.00000002.561422892.00000000040E6000.00000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 00000010.00000002.549878196.00000000034E4000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot	confirm order.exe, 00000000.00000002.447081649.00000000031D1000.00000004.00000800.00020000.00000000.sdmp, confirm order.exe, 00000000.00000002.448397158.0000000003358000.00000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 0000000F.00000002.532893471.00000000029C5000.00000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 0000000F.00000002.532813764.00000000029BC000.00000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 0000000F.00000002.537794657.00000002AEB000.00000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 0000000F.0000002.532109090.0000000002981000.0000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 00000010.00000002.537850084.0000000314B000.00000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 00000010.00000002.532222883.0000000002FE1000.0000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 00000010.00000002.532978281.0000000003025000.00000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 00000010.00000002.532914557.000000000301C000.0000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	confirm order.exe, 0000000E.00000002.532820383.0000000002F41000.00000004.00000800.00020000.00000000.sdmp	false		high
http://james.newtonking.com/projects/json	Ugtphvhf.exe, 00000010.00000002.549878196.00000000034E4000.00000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 00000010.00000002.563075696.000000000417B000.00000004.00000800.00020000.00000000.sdmp, Ugtphvhf.exe, 00000010.00000002.561315549.00000000040DB000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://www.newtonsoft.com/jsonschema	Ugtphvhf.exe, 00000010.00000002.549878196.00000000034E4000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
146.70.76.43	unknown	United Kingdom		2018	TENET-1ZA	true

Private
IP
192.168.2.1

General Information	
Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	712188
Start date and time:	2022-09-29 01:14:32 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	confirm_order.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, 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@11/10@0/2
EGA Information:	• Successful, ratio: 33.3%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings
• Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ocsip.digicert.com, ctldl.windowsupdate.com • Execution Graph export aborted for target Ugtphvhf.exe, PID 5292 because it is empty • Execution Graph export aborted for target confirm_order.exe, PID 5552 because it is empty • Not all processes were analyzed, report is missing behavior information • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations		
Behavior and APIs		
Time	Type	Description
01:15:48	API Interceptor	75x Sleep call for process: powershell.exe modified
01:16:55	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Ugtphvhf "C:\Users\user\AppData\Roaming\Prqhnsx\Ugtphvhf.exe"
01:17:01	API Interceptor	259x Sleep call for process: confirm_order.exe modified
01:17:03	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Ugtphvhf "C:\Users\user\AppData\Roaming\Prqhnsx\Ugtphvhf.exe"

Joe Sandbox View / Context

IPs

 No context

Domains

 No context

ASNs

 No context

JA3 Fingerprints

 No context

Dropped Files

 No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\confirm order.exe.log 

Process:	C:\Users\user\Desktop\confirm order.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1039
Entropy (8bit):	5.3436815157474165
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhyE4KdE4KBLWE4K5AE4Kzr7a:MxHKXwYHKhQnoyHKdHKBqHK5AHKzva
MD5:	6C24176D343957C767AA6536571797FA
SHA1:	64512F67A49AF75E9A67474DF54FCCD3472905B2
SHA-256:	63AB82B5B458425DB1E0831E1BB8CA642C602D9BCB0762A1E47C7836CACF3350
SHA-512:	D0DFB30B723CC1F0ADB8D9448220AC67A1A21243499B7EB31402CAA0CE9F6A892073E10C52D132E59BF2321F05DBB0973B7E1026023992FC33DE5AB74A6979A4
Malicious:	true
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"System.Numerics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime\eb92aa12#34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b880

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5829
Entropy (8bit):	4.8968676994158
Encrypted:	false
SSDEEP:	96:WCJ2Woe5o2k6Lm5emmXIGvgyg12jDs+un/iQLEYFjDaeWJ6KGcmXx9smyFRLcU6f:5xoe5oVsm5emd0gkjDt4iWN3yBGHh9s6
MD5:	36DE9155D6C265A1DE62A448F3B5B66E
SHA1:	02D21946CBDD01860A0DE38D7EEC6CDE3A964FC3

SHA-256:	8BA38D55AA8F1E4F959E7223FDF653ABB9BE5B8B5DE9D116604E1ABB371C1C87
SHA-512:	C734ADE161FB89472B1DF9B9F062F4A53E7010D3FF99EDC0BD564540A56BC35743625C50A00635C31D165A74DCDBB330FFB878C5919D7B267F6F33D2AAB328f7
Malicious:	false
Preview:	PSMODULECACHE.....<e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ...Find-Module.....Find-RoleCapability.....Publish-Script.....<e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*..Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	16496
Entropy (8bit):	5.551918786062227
Encrypted:	false
SSDEEP:	384:cte/cX0w99dEtXt8wnwSBx2u9FiJ9giSJ3uzp1UYv:cEvTZw4cu9picudv
MD5:	88C6EE654500840B8E087B519FBE988D
SHA1:	E28F65A25C048A90228F9EDF8C4A2DE4F35F2A6C
SHA-256:	63C122DE2BA73E9F2CE94D48F4D9F1459BC1638C964B491504E9814FA1A3319E
SHA-512:	FCD7A9867AB7EA689B84F73D4D61F2B1C6216458AB3A62BE712FA8B629FD6C793B50BB0D90D366469F29C62A2CFD50DC25096E5883F90B000200EBB2D7E258C3
Malicious:	false
Preview:	@...e.....:c.....@.....H.....<@^L."My...'. Microsoft.PowerShell.ConsoleHostD.....fZve...F....x.).....System.Management.Automation4.....[...{a.C.%6..h.....System.Core.0.....G-.O...A...4B.....System..4.....Zg5...O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microso ft.Management.Infrastructure.8.....'.L.}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....Syste m.Management...4.....].D.E.....System.Data.H.....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z>..m.....System.Trans actions.<.....):gK..G...\$.1.q.....System.ConfigurationP...../C..J..%...].....%.Microsoft.PowerShell.Commands.Utility..D.....-D.F.<.;nt.1.....Sy stem.Configuration.Ins

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_5zzuyba\sto.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_dygoxbst.ufu.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp_P5ScriptPolicyTest_f2arnmm1.jms.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp_P5ScriptPolicyTest_yxgpc1x.l0u.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat 	
Process:	C:\Users\user\Desktop\confirm order.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:R:R
MD5:	AB8F38A645A923E8D95756E195EEACD1
SHA1:	6BFB7C2285D899A581993B3BAC912375BD55E71D
SHA-256:	0DC4B51B1A57A5DACD962B5FC7C7F52468E5C6861D9D9FD510272723AF26F567
SHA-512:	D266ADB99DFB589F5D13F3E6822EF8395DB557B5DF9B8B990DC957AF07253DAC32EA15147879E11E8FDBA32E536A0EF26D769F6C642D79427C6BCF6C3072EA1
Malicious:	true
Preview:	.q...H

C:\Users\user\AppData\Roaming\Prqhnsx\Ugtphvhf.exe  	
Process:	C:\Users\user\Desktop\confirm order.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	983552
Entropy (8bit):	7.692774803542058
Encrypted:	false
SSDEEP:	24576:7iqfFNQValo1AMQJ2ySwNvxRoi+EGbl5eOR:7iqvyYKMdyS6vxj+Ern
MD5:	E5E6A926238DFECD931967194FF92BF4
SHA1:	B232228269367904BB0EE23B0B47FABF50BA5DF2

SHA-256:	219EEB73337CB0CB6B1E4AF6093AF3C0F4BEF72AF443BE61ADF1B2DC7EAF9063
SHA-512:	A08A5E0A58981A77108AED095F5CCA7B37565EA470079DC6E7F4D462633D080421387159E885E20001F7AD9B28E73E62FC6021A450B543EC61FD19D63F160C79
Malicious:	true
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: ReversingLabs, Detection: 40% - Antivirus: Virustotal, Detection: 49%, Browse
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.PE..L.....0.....@....@..`..... ..@.....-..O..@.....@.....H.....text.....`..rsrc.....@.....@.....@.....@.....rel oc.....@.....@..B.....-.....H.....!.....(....*~s...s...s...((...(*..(*..0..+.....%.....((...%&...-s...z...0.. 0.....(....o....O....s.....Zb.0.....O.....*.....\$.....((...*.0.....s.....+.....(.....[.....].....a.o.....X.....i2.o.....%-&.*B(....r...po....*B(....(....o....*..(....*Fs...%({....}*s...%{.....t....r.. ..po ...ri..po!..})....*..(....*R.{...t".....o"....&*..(....*.BSJB...

C:\Users\user\AppData\Roaming\Prqhnsx\Ugtphvhf.exe:Zone.Identifier 	
Process:	C:\Users\user\Desktop\confirm order.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	true
Preview:	[ZoneTransfer]....Zoneld=0

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.692774803542058
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% - Win16/32 Executable Delphi generic (2074/23) 0.01% - Generic Win/DOS Executable (2004/3) 0.01%
File name:	confirm order.exe
File size:	983552
MD5:	e5e6a926238dfecd931967194ff92bf4
SHA1:	b233228269367904bb0ee23b0b47fabf50ba5df2
SHA256:	219eeb73337cb0cb6b1e4af6093af3c0f4bef72af443be61adf1b2dc7eaf9063
SHA512:	a08a5e0a58981a77108aed095f5cca7b37565ea470079dc6e7f4d462633d080421387159e885e20001f7ad9b28e73e62fc6021a450b543ec61fd19d63f160c79
SSDEEP:	24576:7iqfFNQValo1AMQJ2ySwNvxrRoi+EGbl5eOR:7iqvyYKMdyS6vxj+Ern
TLSH:	6C25E1643D0C075AEACD0EB69E0057DE4EEE5D9F2E384F44BBC09EFE66425D621C0A49
File Content Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.PE..L.....0.....@....@..`.....@.....

File Icon	
	
Icon Hash:	f8d8d0f0c0d0c0c0

Static PE Info	
General	
Entrypoint:	0x402e0e
Entrypoint Section:	.text
Digitally signed:	false

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xDA13C204 [Sun Dec 9 09:19:00 2085 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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]
sbb al, 2Fh

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2dbc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc4000	0x2ebdc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x2da0	0x1c	.text
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	0xc1014	0xc1200	False	0.8617579389158576	SysEx File -	7.847324790581247	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE , IMAGE_SCN_MEM_READ
.rsrc	0xc4000	0x2ebdc	0x2ec00	False	0.34225643382352944	data	5.865926020313647	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf4000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_DISCARD ABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_ICON	0xc4200	0x6c1c	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xcae2c	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 67584		
RT_ICON	0xdb664	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 38016		
RT_ICON	0xe4b1c	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 21600		

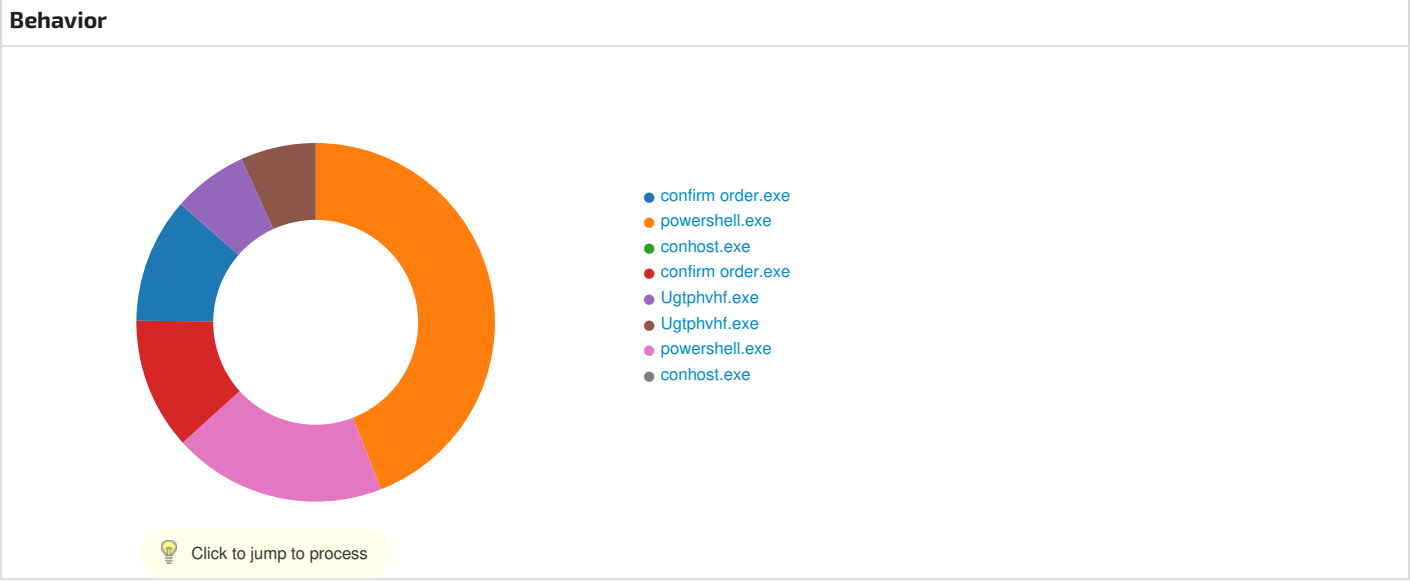
Name	RVA	Size	Type	Language	Country
RT_ICON	0xe9fb4	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16896		
RT_ICON	0xee1ec	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600		
RT_ICON	0xf07a4	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224		
RT_ICON	0xf185c	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400		
RT_ICON	0xf21f4	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088		
RT_GROUP_ICON	0xf266c	0x84	data		
RT_VERSION	0xf2700	0x2dc	data		
RT_MANIFEST	0xf29ec	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports	
DLL	Import
mscorlib.dll	_CorExeMain

Network Behavior

TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 29, 2022 01:17:04.084417105 CEST	49704	56281	192.168.2.3	146.70.76.43
Sep 29, 2022 01:17:07.096297979 CEST	49704	56281	192.168.2.3	146.70.76.43
Sep 29, 2022 01:17:13.112474918 CEST	49704	56281	192.168.2.3	146.70.76.43
Sep 29, 2022 01:17:24.277153015 CEST	49705	56281	192.168.2.3	146.70.76.43
Sep 29, 2022 01:17:27.426295042 CEST	49705	56281	192.168.2.3	146.70.76.43
Sep 29, 2022 01:17:33.426664114 CEST	49705	56281	192.168.2.3	146.70.76.43
Sep 29, 2022 01:17:44.852468014 CEST	49706	56281	192.168.2.3	146.70.76.43
Sep 29, 2022 01:17:47.912234068 CEST	49706	56281	192.168.2.3	146.70.76.43
Sep 29, 2022 01:17:53.912755966 CEST	49706	56281	192.168.2.3	146.70.76.43

Statistics



System Behavior

Analysis Process: confirm order.exe PID: 5552, Parent PID: 6092

General

Target ID:	0
Start time:	01:15:28
Start date:	29/09/2022
Path:	C:\Users\user\Desktop\confirm order.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\confirm order.exe"
Imagebase:	0xdd0000
File size:	983552 bytes
MD5 hash:	E5E6A926238DFECD931967194FF92BF4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.447081649.00000000031D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.447887037.00000000032BD000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth - Rule: NanoCore, Description: unknown, Source: 00000000.00000002.447887037.00000000032BD000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@technanarchy.net> - Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.447887037.00000000032BD000.00000004.00000800.00020000.00000000.sdmp, Author: unknown - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.454452204.0000000004322000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.454452204.0000000004322000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000000.00000002.454452204.0000000004322000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@technanarchy.net> - Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.454452204.0000000004322000.00000004.00000800.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.454858923.0000000005650000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.262094119.0000000004475000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.453904454.0000000004283000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.453904454.0000000004283000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000000.00000002.453904454.0000000004283000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@technanarchy.net> - Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.453904454.0000000004283000.00000004.00000800.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.260970859.00000000041F6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.448397158.0000000003358000.00000004.00000800.00020000.00000000.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	6D37CF06	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	6D37CF06	unknown
C:\Users\user\AppData\Roaming\Prqhnsx	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6C1CBEFF	CreateDirectoryW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\confirm order.exe.log	0	1039	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","N otApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6D68C907	WriteFile

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D355705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D355705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D35CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D355705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D355705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#34957343ad5d84dae97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D2B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\1b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2B03DE	ReadFile	

Registry Activities							
Key Value Created							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsof\Windows\CurrentVersion\Run	Ugtphvhf	unicode	"C:\Users\user\AppData\Roaming\Prqhnsx\Ugtphvhf.exe"	success or wait	1	6C1C646A	RegSetValueExW

Analysis Process: powershell.exe PID: 1756, Parent PID: 5552	
General	
Target ID:	1
Start time:	01:15:41
Start date:	29/09/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACA ANgAwAA==

Imagebase:	0x10000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_5zzuybal.sto.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6C1C1E60	CreateFileW	
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_dygoxst.ufu.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6C1C1E60	CreateFileW	
C:\Users\user\AppData\Local\Mi crosoft\Windows\PowerShell\ModuleAnalysisCache	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	6C1C1E60	CreateFileW	
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	6D37CF06	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	6D37CF06	unknown	

File Deleted					
File Path	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5zzuybal.sto.ps1	success or wait	1	6C1C6A95	DeleteFileW	
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dygoxst.ufu.psm1	success or wait	1	6C1C6A95	DeleteFileW	

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C125B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C125B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C125B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C125B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C125B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C125B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C125B28	unknown
C:\Users\user\AppData\Local\Te mp__PSscr iptPolicyTest_5zzuybal.sto.ps1	0	1	31	1	success or wait	1	6C1C1B4F	WriteFile
C:\Users\user\AppData\Local\Te mp__PSscr iptPolicyTest_dygoxst.ufu.psm1	0	1	31	1	success or wait	1	6C1C1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE<eY C:\Program Files (x86)\WindowsPowerShell ModuleAnalysisCache PowerShellGet\1.0.0 .1\PowerShellGet.psd1Uninstall- ModuleinmofimolInstall- ModuleNew-scriptFileInfoPublish- ModuleInstall-ScriptFileInfoPublish-	success or wait	1	6C1C1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	1733	00 0a 00 00 00 47 65 74 2d 52 61 6e 64 6f 6d 08 00 00 00 03 00 00 00 43 46 53 01 00 00 00 0a 00 00 00 4f 75 74 2d 53 74 72 69 6e 67 08 00 00 00 0e 00 00 00 57 72 69 74 65 2d 50 72 6f 67 72 65 73 73 08 00 00 00 14 00 00 00 44 69 73 61 62 6c 65 2d 50 53 42 72 65 61 6b 70 6f 69 6e 74 08 00 00 00 11 00 00 00 55 70 64 61 74 65 2d 46 6f 72 6d 61 74 44 61 74 61 08 00 00 00 11 00 00 00 57 72 69 74 65 2d 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 43 6f 6e 76 65 72 74 54 6f 2d 58 6d 6c 08 00 00 00 0c 00 00 00 53 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0b 00 00 00 4f 75 74 2d 50 72 69 6e 74 65 72 08 00 00 00 fd fd fd fd 79 48 fd 38 9f fd 08 49 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50	Get-RandomCFSOutput-StringWrite-ProgressDisable-PSBreakpointUpdate-FormatDataWrite-InformationConvertTo-XmlSet-VariableOutput-PrinterYH8IC:\Program Files (x86)\WindowsPowerShell\PowerShellGet\1.0.0\PowerShellGet.psd1Uninstall-ModuleinmofimolInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-ScriptFileInfoPublish-	success or wait	1	6C1C1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 0f 00 00 00 08 0f 00 00 11 00 00 00 fd 0e fd 05 fd 08 fd 08 02 08 00 00 3a 01 63 00 09 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e:c@	success or wait	1	6D6476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 27 00 00 00 0e 00 20 00	H<@^L"My:'	success or wait	15	6D6476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	15	6D6476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	6D6476FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	00 08 00 03		success or wait	8	6D6476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 54 01 40 00 fd 3e 40 01 09 0c fd 00 58 64 40 01 56 64 40 01 fd 2a 40 01 fd 00 00 00 56 01 00 00 48 01 00 00 58 01 00 00 5b 01 00 00 4e 54 00 01 48 54 00 01 fd 53 00 01 fd 53 00 01 68 54 00 01 fd 53 00 01 fd 53 00 01 5c 01 00 00 00 54 00 01 02 54 00 01 40 58 00 01 3f 58 00 01 1c 54 00 01 fd 53 00 01 fd 53 00 01 1e 54 00 01 19 54 00 01 78 54 00 01 7a 54 00 01 fd 54 00 01 3d 4d 00 01 44 4d 00 01 3a 4d 00 01 22 4d 00 01 20 4d 00 01 21 4d 00 01 3b 4d 00 01 fd 44 00 01 fd 44 00 01 40 4d 00 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 16 3b 00 01 1b 3b 00 01 19 3b 00 01 fd 3c 00 01 fd 3c 00 01 fd 3c 00 01 57 03 00 01 4d 03 00 01 fd 45 00	T@>@Xd@Vd@*@VHX [NTHtSShTSSS\TT@X? XTSSTTxTzTT=MDM:M" M M!M;MDD @M<M\$M8M?M;;; <<<WME	success or wait	8	6D6476FC	WriteFile

File Read						
File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D355705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D355705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae4ee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2B03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D35CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D35CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D35CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2B03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D355705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D355705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2B03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D355705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D355705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.M49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D2B03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D361F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22412	success or wait	1	6D36203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2B03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C1C1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	122	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C1C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C1C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C1C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C1C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C1C1B4F	ReadFile

Analysis Process: conhost.exe PID: 1652, Parent PID: 1756

General

Target ID:	2
Start time:	01:15:41

Start date:	29/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: confirm order.exe PID: 1020, Parent PID: 5552

General	
Target ID:	14
Start time:	01:16:58
Start date:	29/09/2022
Path:	C:\Users\user\Desktop\confirm order.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\confirm order.exe
Imagebase:	0x9b0000
File size:	983552 bytes
MD5 hash:	E5E6A926238DFECD931967194FF92BF4
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: 0000000E.00000000.444492363.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000000.444492363.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000000.444492363.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@technarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000E.00000000.444492363.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.549837955.0000000005830000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.549837955.0000000005830000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000E.00000002.549837955.0000000005830000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000E.00000002.549837955.0000000005830000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.550441938.0000000006010000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.550441938.0000000006010000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.550441938.0000000006010000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000E.00000002.550441938.0000000006010000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000E.00000002.550441938.0000000006010000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.532820383.0000000002F41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.532820383.0000000002F41000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@technarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000E.00000002.532820383.0000000002F41000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.545716802.0000000003F72000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.545716802.0000000003F72000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@technarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000E.00000002.545716802.0000000003F72000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6D37CF06	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	6D37CF06	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	6C1CBEFF	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	6C1C1E60	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	6C1CBEFF	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	6C1CBEFF	CreateDirectoryW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	96 71 fd fd fd 48	qH	success or wait	1	6C1C1B4F	WriteFile

File Read						
File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D355705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D35CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Users\user\Desktop\confirm order.exe	unknown	4096	success or wait	1	6D33D72F	unknown
C:\Users\user\Desktop\confirm order.exe	unknown	512	success or wait	1	6D33D72F	unknown

Analysis Process: Ugtphvhf.exe PID: 5292, Parent PID: 3452	
General	
Target ID:	15
Start time:	01:17:03

Start date:	29/09/2022
Path:	C:\Users\user\AppData\Roaming\Prqhnsx\Ugtphvhf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Prqhnsx\Ugtphvhf.exe"
Imagebase:	0x510000
File size:	983552 bytes
MD5 hash:	E5E6A926238DFECD931967194FF92BF4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000F.00000002.532813764.00000000029BC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000F.00000002.532893471.00000000029C5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000F.00000002.532109090.0000000002981000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000F.00000002.537794657.0000000002AEB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	- Detection: 100%, Joe Sandbox ML - Detection: 40%, ReversingLabs - Detection: 49%, Virustotal, Browse
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	6D37CF06	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	6D37CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D355705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D35CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.4f0a7eefa3cd3e0ba98b5ebddb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D355705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime.92aa12#34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2B03DE	ReadFile

Analysis Process: Ugtphvhf.exe PID: 6072, Parent PID: 3452

General

Target ID:	16
Start time:	01:17:12
Start date:	29/09/2022
Path:	C:\Users\user\AppData\Roaming\Prqhnsx\Ugtphvhf.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\AppData\Roaming\Prqhnsx\Ugtphvhf.exe"
Imagebase:	0xb30000
File size:	983552 bytes
MD5 hash:	E5E6A926238DFECD931967194FF92BF4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000010.00000002.532222883.0000000002FE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000010.00000002.537850084.000000000314B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000010.00000002.532914557.000000000301C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000010.00000002.532978281.0000000003025000.00000004.00000800.00020000.00000000.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	6D37CF06	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	6D37CF06	unknown	

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D355705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D355705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D35CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D355705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D355705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D2B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\1b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2B03DE	ReadFile	

Analysis Process: powershell.exe PID: 5344, Parent PID: 5292	
General	
Target ID:	17
Start time:	01:17:24
Start date:	29/09/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcbB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANgAwAA==
Imagebase:	0x10000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Temp__PSscrip tPolicyTest_yxgpca1x.l0u.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6C1C1E60	CreateFileW	
C:\Users\user\AppData\Local\Temp__PSscrip tPolicyTest_f2arnmm1.jms.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6C1C1E60	CreateFileW	

File Deleted				
File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscrip tPolicyTest_yxgpca1x.l0u.ps1	success or wait	1	6C1C6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscrip tPolicyTest_f2arnmm1.jms.psm1	success or wait	1	6C1C6A95	DeleteFileW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Te mp__PSscri tPolicyTest_yxgpca1x.l0u.ps1	0	1	31	1	success or wait	1	6C1C1B4F	WriteFile
C:\Users\user\AppData\Local\Te mp__PSscri tPolicyTest_f2arnmm1.jms.psm1	0	1	31	1	success or wait	1	6C1C1B4F	WriteFile

File Read								
File Path	Offset	Length	Completion	Count	Source Address	Symbol		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D355705	unknown		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D355705	unknown		
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D355705	unknown		
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D355705	unknown		
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152 fe02a317a77ae4ee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2B03DE	ReadFile		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D35CA54	ReadFile		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D35CA54	ReadFile		
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D35CA54	ReadFile		
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1 d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2B03DE	ReadFile		
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2B03DE	ReadFile		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D355705	unknown		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D355705	unknown		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D355705	unknown		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D355705	unknown		
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2B03DE	ReadFile		
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Managemen t.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D2B03DE	ReadFile		
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	unknown	64	success or wait	1	6D361F73	ReadFile		
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	unknown	16432	success or wait	1	6D36203F	ReadFile		
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuratio n.ni.dll.aux	unknown	864	success or wait	1	6D2B03DE	ReadFile		
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Mod uleAnalysisCache	unknown	4096	success or wait	1	6C1C1B4F	ReadFile		
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Mod uleAnalysisCache	unknown	1	success or wait	1	6C1C1B4F	ReadFile		

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C1C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	3	6C1C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C1C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C1C1B4F	ReadFile

Analysis Process: conhost.exe PID: 2384, Parent PID: 5344

General

Target ID:	18
Start time:	01:17:24
Start date:	29/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7f745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly