ID: 341280
Sample Name: Order list 20.1.2021 07u9Uxttb5ltGU.exe
Cookbook: default.jbs
Time: 07:49:49
Date: 19/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

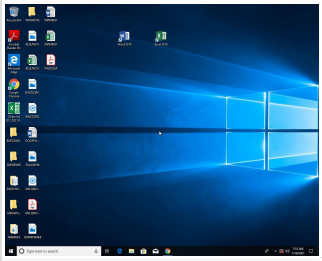
Analysis Report Order list 20.1.2021 07u9Uxttb5ltGU.exe

Overview

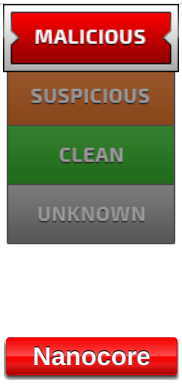
General Information

Sample Name:	Order list 20.1.2021 07u9Uxttb5ltGU.exe
Analysis ID:	341280
MD5:	8935c408c56501..
SHA1:	69fbb8236dc9583.
SHA256:	5fc84f25b331a01..
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection



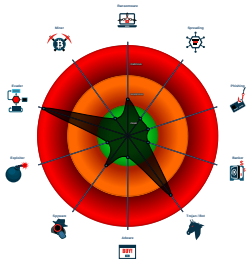
Nanocore

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

Signatures

- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- Order list 20.1.2021 07u9Uxttb5ltGU.exe (PID: 6148 cmdline: 'C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.exe' MD5: 8935C408C5650172E350ACB92E7CC659)
  - schtasks.exe (PID: 6124 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\gIZSEI' /XML 'C:\Users\user\AppData\Local\Temp\tmpE60F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4612 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Order list 20.1.2021 07u9Uxttb5ltGU.exe (PID: 5040 cmdline: C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.exe MD5: 8935C408C5650172E350ACB92E7CC659)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.662843036.000000000276B000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.664198703.0000000003F65000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x365ee5:$x1: NanoCore.ClientPluginHost • 0x398705:$x1: NanoCore.ClientPluginHost • 0x365f22:$x2: IClientNetworkHost • 0x398742:$x2: IClientNetworkHost • 0x369a55:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x39c275:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000002.664198703.0000000003F65000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.664198703.0000000003F65000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x365c4d:$a: NanoCore • 0x365c5d:$a: NanoCore • 0x365e91:$a: NanoCore • 0x365ea5:$a: NanoCore • 0x365ee5:$a: NanoCore • 0x39846d:$a: NanoCore • 0x39847d:$a: NanoCore • 0x3986b1:$a: NanoCore • 0x3986c5:$a: NanoCore • 0x398705:$a: NanoCore • 0x365cac:$b: ClientPlugin • 0x365eae:$b: ClientPlugin • 0x365eee:$b: ClientPlugin • 0x3984cc:$b: ClientPlugin • 0x3986ce:$b: ClientPlugin • 0x39870e:$b: ClientPlugin • 0x20509e:$c: ProjectData • 0x2700be:$c: ProjectData • 0x365dd3:$c: ProjectData • 0x3985f3:$c: ProjectData • 0x3667da:$d: DESCrypto
Process Memory Space: Order list 20.1.2021 07u9Uxt tb5ltGU.exe PID: 6148	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

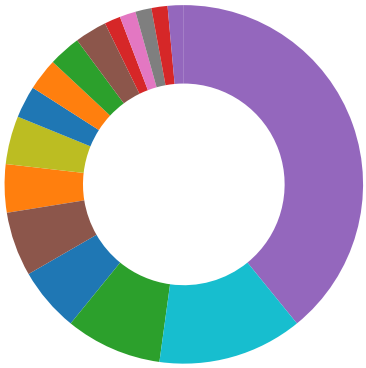
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Compliance:

Detected unpacking (overwrites its own PE header)

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

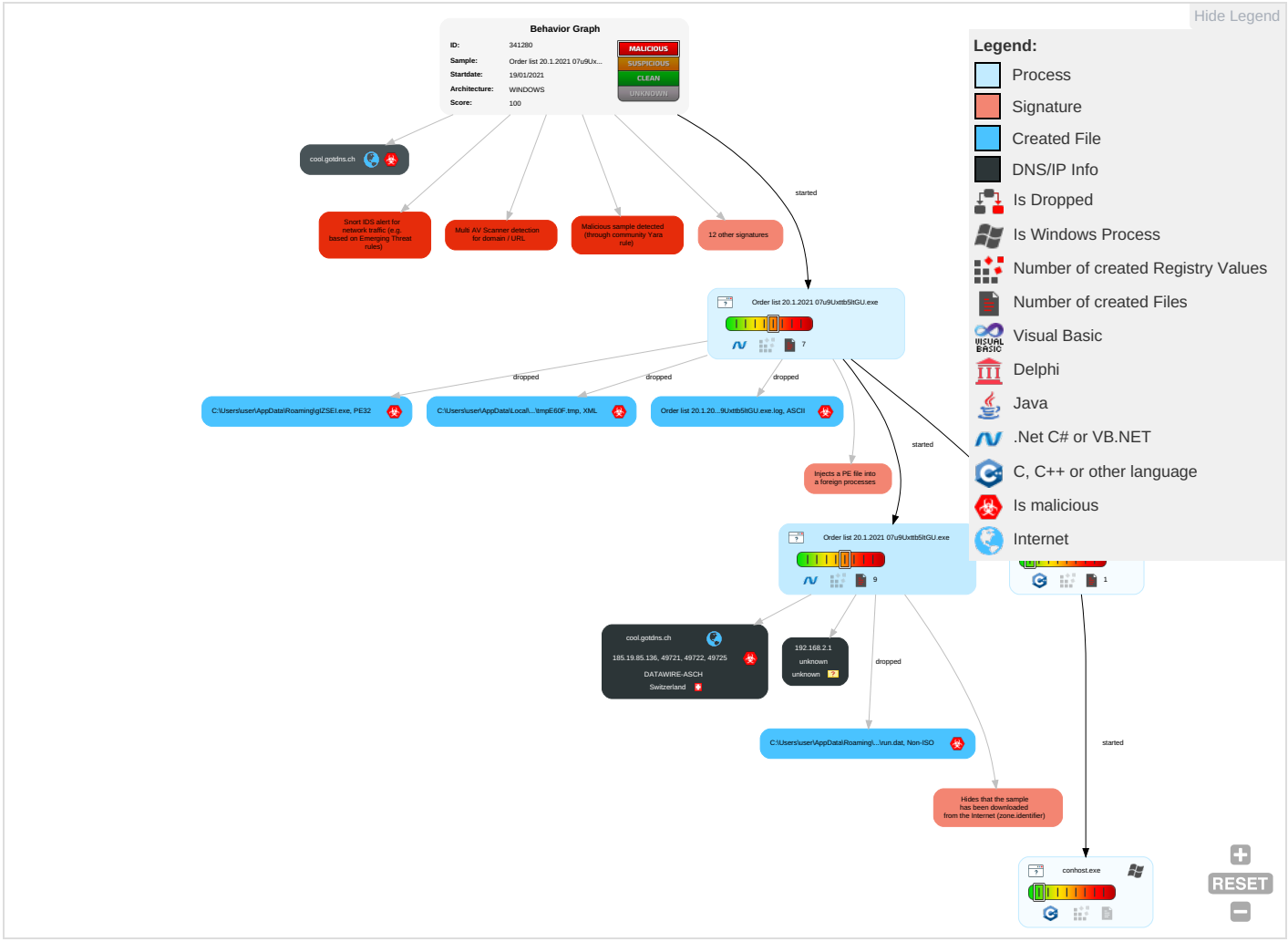
Yara detected Nanocore RAT

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	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effects
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Security Software Discovery 2 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit Track I Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2 1	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

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 list 20.1.2021 07u9Uxttb5ltGU.exe	14%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\gIZSEI.exe	14%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.Order list 20.1.2021 07u9Uxttb5ltGU.exe.f0000.0.unpack	100%	Avira	HEUR/AGEN.1134873		Download File

Domains

Source	Detection	Scanner	Label	Link
cool.gotdns.ch	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/DataSet.xsd	0%	Avira URL Cloud	safe	

Domains and IPs

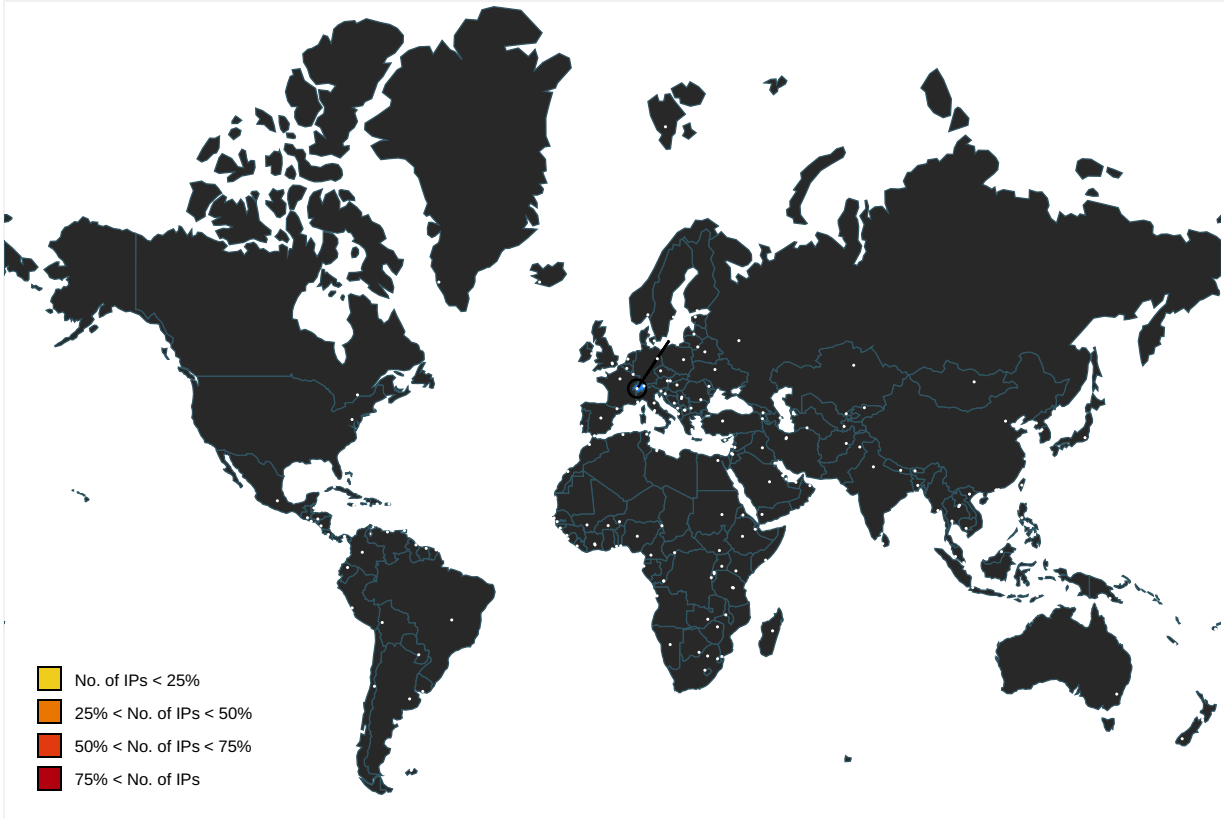
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cool.gotdns.ch	185.19.85.136	true	true	• 8%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Order list 20.1.2021 07u9Uxttb5ltGU.exe, 00000001.00000002.662843036.000000000276B000.00000004.00000001.sdmp	false		high
http://tempuri.org/DataSet.xsd	Order list 20.1.2021 07u9Uxttb5ltGU.exe, 00000001.00000002.662843036.000000000276B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.19.85.136	unknown	Switzerland		48971	DATAWIRE-ASCH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	341280
Start date:	19.01.2021
Start time:	07:49:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Order list 20.1.2021 07u9Uxttb5ltGU.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/8@26/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.3% (good quality ratio 1%) • Quality average: 32% • Quality standard deviation: 39%
HCA Information:	• Successful, ratio: 99% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 104.43.139.144, 51.104.139.180, 92.122.213.194, 92.122.213.247, 2.20.142.210, 2.20.142.209, 52.254.96.93, 20.54.26.129, 52.147.198.201, 13.64.90.137, 52.255.188.83 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, bn2eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.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 NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:50:39	API Interceptor	1431x Sleep call for process: Order list 20.1.2021 07u9Uxttb5ltGU.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.19.85.136	DHL AWD 3374687886,pdf.exe	Get hash	malicious	Browse	
	Documento AWB DHL 3374687886.exe	Get hash	malicious	Browse	
	DHL 3374687886,PDF.exe	Get hash	malicious	Browse	
	Shipping Document PL& BL 960.exe	Get hash	malicious	Browse	
	Gitco_Inquiry _List.exe	Get hash	malicious	Browse	
	HMPEX_PO201120112.exe	Get hash	malicious	Browse	
	Unimac_Project_ORDER 10177_R29.exe	Get hash	malicious	Browse	
	Y4Taap3cTy.exe	Get hash	malicious	Browse	
	JEmT3ndkrV.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DATAWIRE-ASCH	FACTURAS-1-2021.vbs	Get hash	malicious	Browse	• 185.19.85.143
	DHL AWD 3374687886,pdf.exe	Get hash	malicious	Browse	• 185.19.85.136
	Documento AWB DHL 3374687886.exe	Get hash	malicious	Browse	• 185.19.85.136
	xpmcQRN870.exe	Get hash	malicious	Browse	• 185.19.85.135
	Pokana2021011357.doc	Get hash	malicious	Browse	• 185.19.85.135
	DHL 3374687886,PDF.exe	Get hash	malicious	Browse	• 185.19.85.136
	Shipping Document PL& BL 960.exe	Get hash	malicious	Browse	• 185.19.85.136
	CERERE DE COTARE.exe	Get hash	malicious	Browse	• 185.19.85.153
	NEW ORDERS.exe	Get hash	malicious	Browse	• 185.19.85.146
	PO#5176866.exe	Get hash	malicious	Browse	• 185.19.85.153
	Remittance.exe	Get hash	malicious	Browse	• 185.19.85.133
	i_Remittance.exe	Get hash	malicious	Browse	• 185.19.85.133
	vale-remittance.exe	Get hash	malicious	Browse	• 185.19.85.133
	Gitco_Inquiry _List.exe	Get hash	malicious	Browse	• 185.19.85.136
	2020RFQ48839957375883758877.exe	Get hash	malicious	Browse	• 185.19.85.155
	PO-IMG-00WDE21-00SW12-1102DD.exe	Get hash	malicious	Browse	• 185.19.85.183
	RemittanceCopy.js	Get hash	malicious	Browse	• 185.19.85.181
	Gray_Sample_pictures001029D7FE46G.exe	Get hash	malicious	Browse	• 185.19.85.183
	HMPEX_PO201120112.exe	Get hash	malicious	Browse	• 185.19.85.136
	MC20200603.exe	Get hash	malicious	Browse	• 185.19.85.149

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order list 20.1.2021 07u9Uxttb5ltGU.exe.log

Process:	C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmpE60F.tmp

Process:	C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.1752158804126145

C:\Users\user\AppData\Local\Temp\tmpE60F.tmp	
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGPtn:cbhK79lNQR/rydbz9I3YODOLNdq32
MD5:	26FDC12F4303E1CE02877707F93D1711
SHA1:	E48011B6254C2B4689027136EA674E8560E6E371
SHA-256:	555888AB668D8D97930E68EF519AD14F4ACA94562210A1EFB2BAF09C86512B14
SHA-512:	FDB839496AF269748BED58D1215144494CA96CA06696A8D677CAC306D25030BC2F3209E02072DCBFF71695440BC03877F9F2356B2CD02798F5C0CA18B27DD32
Malicious:	**true**
Reputation:	low
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>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.exe
File Type:	data
Category:	dropped
Size (bytes):	1392
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	24:IQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUt4:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/f
MD5:	E78C6686C5A1A9CB0724F84DEA9A75F0
SHA1:	80E61D5BDC7AF293362024781DA66BEA9D370FF9
SHA-256:	FBE0B513511C00AC3B7169E1BCFB675CFD708B249365D724269C23FAC1184967
SHA-512:	FF3835238CAEA26D8800B56901AB962ACD2FA390F955C4A8A15B5817AAB7642D105538CF63938D218567501477FB4B23C2834F22CBC8BA0002C7BCACB2875637
Malicious:	false
Reputation:	low
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:6ujx:Ft
MD5:	D57F6F8719FAFDD38D9BBB21A60AD9E0
SHA1:	547C1104C41BF4E65F0C633D711660B39D23C553
SHA-256:	2C684325E720A99735382667245820FC61C73CE32BE40C4BA78EA80971A3CFCF
SHA-512:	5438C76F099D073A3AF8951B26DE379276CB1C95CF99F88AD3DAAE6DF7687000B848151E5DD22CA5BC6C6E1110B1B51DC081EE07AF9AEF42F251A314EBA338 9
Malicious:	**true**
Reputation:	low
Preview:	...F..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'..}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\gIZSEI.exe	
Process:	C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1741312
Entropy (8bit):	7.044200529220029
Encrypted:	false
SSDEEP:	24576:RJEl7t/bYfqiY11a8gPgYUGwTNIg7Esbz1A6bagTRyvN:7ElBzYfqiww9gYUnTOcEsf1XJTR
MD5:	8935C408C5650172E350ACB92E7CC659
SHA1:	69FBB8236DC958388BDAF65B986894365D6DAE6B
SHA-256:	5FC84F25B331A01C87E4F7652A396A83403C0EFC27CEFEEC6CEA69B954A01040
SHA-512:	55312234692BBD6E2B60128350A32E02D2D8AFFBAA154280B5F080044039F14660114483BAAF81BAA940122AA4B04A7A247CA5DF02EF7CA993D287B8C6DFDD5E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 14%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....*.`.....P..... .....@.. ..... ..@.....W..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....(>.....B....4.....w|E~}l....J.b.NtF...e.:..%.....:...w.....^.V.3l.....u.....1.....1x....t..3.3n..`S.l.e...lDT.4[.2?... o.U...@G..h..et..8..3..A.n....k...Z....QQ7.....H.....N(V...G.V.{.?...N.P+6...?.=.C...rU;....Wv.Js...2q.zh.C....!....;]..0.....~._.O..AsD:...pZ.H.....eD...?.Pds..T.?...p4...Yg.5.....1. 5=.....Y..i.....T...h&.J....z..pa~.UF..HdK.o|..' ..<..A.....}..&u....4..."...A]..K9

C:\Users\user\AppData\Roaming\gIZSEI.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.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:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.044200529220029
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Order list 20.1.2021 07u9Uxttb5ltGU.exe
File size:	1741312
MD5:	8935c408c5650172e350acb92e7cc659
SHA1:	69fbb8236dc958388bdaf65b986894365d6dae6b
SHA256:	5fc84f25b331a01c87e4f7652a396a83403c0efc27cefeec6cea69b954a01040
SHA512:	55312234692bbd6e2b60128350a32e02d2d8affbaa1542 0b5f080044039f14660114483baaf81baa940122aa4b04a 7a247ca5df02ef7ca993d287b8c6dfdd5e
SSDEEP:	24576:RJEl7t/bYfqiY11a8gPgYUGwTNIg7Esbz1A6bagTRyvN:7ElBzYfqiww9gYUnTOcEsf1XJTR
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....*.`.....P..... .....@.. .....@.....

File Icon

Icon Hash:	4fa1acacaca9254f

Static PE Info

General

Entrypoint:	0x58dd0e
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:	0x60062AA5 [Tue Jan 19 00:41:09 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x18dcb4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x18e000	0x1cfd0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1ac000	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	0x18bd14	0x18be00	False	0.613764751737	data	7.07883915605	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x18e000	0x1cfd0	0x1d000	False	0.284979458513	data	5.23332295466	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1ac000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x18e220	0x42aa	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x1924cc	0x10828	dBase III DBT, version number 0, next free block index 40		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1a2cf4	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x1a6f1c	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x1a94c4	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 1089400558, next used block 1089400558		
RT_ICON	0x1aa56c	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1aa9d4	0x5a	data		
RT_VERSION	0x1aaa30	0x3b4	data		
RT_MANIFEST	0x1aade4	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 2019 Principle Pleasure
Assembly Version	7.20.17.0
InternalName	IResourceGroveler.exe
FileVersion	7.20.17.0
CompanyName	
LegalTrademarks	
Comments	Principle Pleasure
ProductName	Record Bgy System
ProductVersion	7.20.17.0
FileDescription	Record Bgy System
OriginalFilename	IResourceGroveler.exe

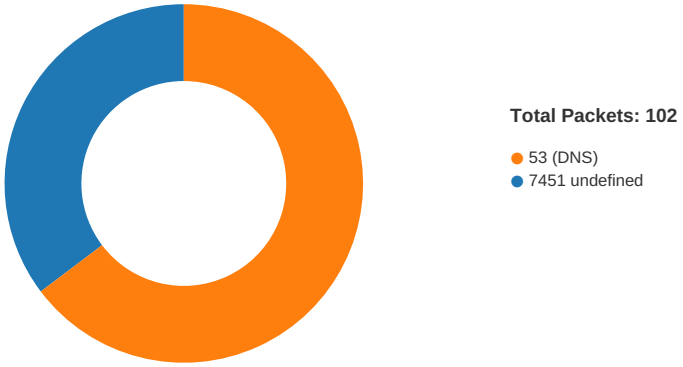
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/19/21-07:50:47.391360	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	7451	192.168.2.4	185.19.85.136
01/19/21-07:50:54.760816	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49722	7451	192.168.2.4	185.19.85.136
01/19/21-07:51:01.352160	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	7451	192.168.2.4	185.19.85.136
01/19/21-07:51:07.310601	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	7451	192.168.2.4	185.19.85.136
01/19/21-07:51:13.744730	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49729	7451	192.168.2.4	185.19.85.136
01/19/21-07:51:20.604711	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	7451	192.168.2.4	185.19.85.136
01/19/21-07:51:27.840868	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	7451	192.168.2.4	185.19.85.136
01/19/21-07:51:34.284086	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	7451	192.168.2.4	185.19.85.136
01/19/21-07:51:41.520045	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	7451	192.168.2.4	185.19.85.136
01/19/21-07:51:47.214796	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	7451	192.168.2.4	185.19.85.136
01/19/21-07:51:53.279687	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	7451	192.168.2.4	185.19.85.136
01/19/21-07:52:00.336225	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	7451	192.168.2.4	185.19.85.136
01/19/21-07:52:06.320462	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	7451	192.168.2.4	185.19.85.136

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/19/21-07:52:13.317495	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49764	7451	192.168.2.4	185.19.85.136
01/19/21-07:52:18.262032	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	7451	192.168.2.4	185.19.85.136
01/19/21-07:52:25.288563	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49776	7451	192.168.2.4	185.19.85.136
01/19/21-07:52:31.305836	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	7451	192.168.2.4	185.19.85.136
01/19/21-07:52:37.275244	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	7451	192.168.2.4	185.19.85.136
01/19/21-07:52:44.259420	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	7451	192.168.2.4	185.19.85.136
01/19/21-07:52:51.314375	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49780	7451	192.168.2.4	185.19.85.136
01/19/21-07:52:57.513870	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49781	7451	192.168.2.4	185.19.85.136
01/19/21-07:53:04.457835	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49782	7451	192.168.2.4	185.19.85.136
01/19/21-07:53:11.456831	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	7451	192.168.2.4	185.19.85.136
01/19/21-07:53:17.525829	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49784	7451	192.168.2.4	185.19.85.136
01/19/21-07:53:24.554457	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	7451	192.168.2.4	185.19.85.136

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 07:50:47.200128078 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:47.344275951 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:47.344770908 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:47.391360044 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:47.596051931 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:47.596093893 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:47.609293938 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:47.755491972 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:47.793704987 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:47.986874104 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:47.987035990 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.100265980 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.100301027 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.100366116 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.100408077 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.100434065 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.100461960 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.100496054 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.102679968 CET	49721	7451	192.168.2.4	185.19.85.136

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 07:50:48.142199039 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.240861893 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.240906954 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.241035938 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.241056919 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.241188049 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.241420984 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.255206108 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.255338907 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.255446911 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.255461931 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.255712986 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.255772114 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.363406897 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.363503933 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.363585949 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.363617897 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.366002083 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.366239071 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.377692938 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.377872944 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.378000021 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.378612041 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.378954887 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.379349947 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.406094074 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.406163931 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.406344891 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.406395912 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.406518936 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.406722069 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.406729937 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.406775951 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.406897068 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.407572031 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.407605886 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.408358097 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.495733023 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.495769024 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.495881081 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.496220112 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.496340036 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.497419119 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.556272030 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.556310892 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.556334972 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.556593895 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.557759047 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.557883024 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.557997942 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.558056116 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.558068991 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.558111906 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.558248043 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.558331013 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.558480024 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.558511019 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.558603048 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.558712006 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.558736086 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.558800936 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.558959007 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.559015989 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.559024096 CET	49721	7451	192.168.2.4	185.19.85.136

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 07:50:48.559727907 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.559993029 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.560117960 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.560200930 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.560220957 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.560322046 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.560439110 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.560456991 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.560600996 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.560666084 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.560684919 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.560800076 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.560919046 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.560939074 CET	49721	7451	192.168.2.4	185.19.85.136
Jan 19, 2021 07:50:48.561043024 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.561160088 CET	7451	49721	185.19.85.136	192.168.2.4
Jan 19, 2021 07:50:48.561250925 CET	49721	7451	192.168.2.4	185.19.85.136

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 07:50:33.439085960 CET	65298	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:50:33.497582912 CET	53	65298	8.8.8.8	192.168.2.4
Jan 19, 2021 07:50:34.822033882 CET	59123	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:50:34.878926039 CET	53	59123	8.8.8.8	192.168.2.4
Jan 19, 2021 07:50:47.090461969 CET	54531	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:50:47.152731895 CET	53	54531	8.8.8.8	192.168.2.4
Jan 19, 2021 07:50:53.973232031 CET	49714	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:50:54.034387112 CET	53	49714	8.8.8.8	192.168.2.4
Jan 19, 2021 07:50:59.614392042 CET	58028	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:50:59.664474964 CET	53	58028	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:01.139107943 CET	53097	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:01.195585012 CET	53	53097	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:04.887340069 CET	49257	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:05.811196089 CET	62389	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:05.875787020 CET	49257	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:06.815979004 CET	62389	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:06.875248909 CET	53	62389	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:06.876454115 CET	49257	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:06.937066078 CET	53	49257	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:07.087359905 CET	49910	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:07.135196924 CET	53	49910	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:13.528394938 CET	55854	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:13.584745884 CET	53	55854	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:20.350526094 CET	64549	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:20.406888962 CET	53	64549	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:21.798362970 CET	63153	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:21.855885029 CET	53	63153	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:22.514637947 CET	52991	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:22.613488913 CET	53	52991	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:23.486267090 CET	53700	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:23.566497087 CET	53	53700	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:23.773998976 CET	51726	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:23.838339090 CET	53	51726	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:24.570322990 CET	56794	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:24.626552105 CET	53	56794	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:25.499701977 CET	56534	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:25.556174994 CET	53	56534	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:26.501979113 CET	56627	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:26.552752018 CET	53	56627	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:27.635762930 CET	56621	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:27.662904978 CET	63116	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:27.694797039 CET	53	56621	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:27.719813108 CET	53	63116	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 07:51:29.231795073 CET	64078	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:29.290724993 CET	53	64078	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:31.755481958 CET	64801	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:31.811820030 CET	53	64801	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:33.436482906 CET	61721	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:33.492866993 CET	53	61721	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:34.058247089 CET	51255	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:34.119842052 CET	53	51255	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:34.372250080 CET	61522	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:34.433628082 CET	53	61522	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:37.465224981 CET	52337	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:37.523499966 CET	53	52337	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:37.844856024 CET	55046	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:37.892827034 CET	53	55046	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:38.699158907 CET	49612	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:38.747292995 CET	53	49612	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:39.525033951 CET	49285	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:39.573904991 CET	53	49285	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:41.164343119 CET	50601	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:41.217613935 CET	53	50601	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:46.980333090 CET	60875	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:47.039541960 CET	53	60875	8.8.8.8	192.168.2.4
Jan 19, 2021 07:51:53.068682909 CET	56448	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:51:53.127065897 CET	53	56448	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:00.094484091 CET	59172	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:00.155435085 CET	53	59172	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:06.075536013 CET	62420	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:06.131798983 CET	53	62420	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:07.854959011 CET	60579	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:07.902884007 CET	53	60579	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:09.874206066 CET	50183	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:09.946219921 CET	53	50183	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:10.103743076 CET	61531	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:10.154392958 CET	53	61531	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:10.950565100 CET	49228	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:11.001297951 CET	53	49228	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:11.879450083 CET	59794	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:11.935806990 CET	53	59794	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:12.763459921 CET	55916	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:12.811623096 CET	53	55916	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:13.109258890 CET	52752	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:13.170758009 CET	53	52752	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:13.538729906 CET	60542	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:13.597917080 CET	53	60542	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:14.342592955 CET	60689	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:14.401134014 CET	53	60689	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:17.065999031 CET	64206	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:17.113924980 CET	53	64206	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:17.869931936 CET	50904	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:17.918083906 CET	53	50904	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:18.079467058 CET	57525	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:18.135664940 CET	53	57525	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:18.747370958 CET	53814	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:18.795670033 CET	53	53814	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:19.614914894 CET	53418	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:19.662883997 CET	53	53418	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:20.412235022 CET	62833	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:20.460144997 CET	53	62833	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:21.187096119 CET	59260	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:21.237788916 CET	53	59260	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:22.171420097 CET	49944	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:22.219074965 CET	53	49944	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:22.950644016 CET	63300	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:22.998507977 CET	53	63300	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 07:52:25.099489927 CET	61449	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:25.155678034 CET	53	61449	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:31.103212118 CET	51275	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:31.159454107 CET	53	51275	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:37.087351084 CET	63492	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:37.149038076 CET	53	63492	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:44.087116957 CET	58945	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:44.143927097 CET	53	58945	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:51.129041910 CET	60779	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:51.177094936 CET	53	60779	8.8.8.8	192.168.2.4
Jan 19, 2021 07:52:57.229067087 CET	64014	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:52:57.288357973 CET	53	64014	8.8.8.8	192.168.2.4
Jan 19, 2021 07:53:04.241309881 CET	57091	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:53:04.297863007 CET	53	57091	8.8.8.8	192.168.2.4
Jan 19, 2021 07:53:11.266027927 CET	55904	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:53:11.328566074 CET	53	55904	8.8.8.8	192.168.2.4
Jan 19, 2021 07:53:17.334252119 CET	52109	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:53:17.392471075 CET	53	52109	8.8.8.8	192.168.2.4
Jan 19, 2021 07:53:24.345340014 CET	54450	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:53:24.403909922 CET	53	54450	8.8.8.8	192.168.2.4
Jan 19, 2021 07:53:29.325831890 CET	49374	53	192.168.2.4	8.8.8.8
Jan 19, 2021 07:53:29.384881020 CET	53	49374	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 19, 2021 07:50:47.090461969 CET	192.168.2.4	8.8.8.8	0xdb52	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:50:53.973232031 CET	192.168.2.4	8.8.8.8	0x4dc3	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:01.139107943 CET	192.168.2.4	8.8.8.8	0x5504	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:07.087359905 CET	192.168.2.4	8.8.8.8	0xd323	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:13.528394938 CET	192.168.2.4	8.8.8.8	0x8d5a	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:20.350526094 CET	192.168.2.4	8.8.8.8	0xd67b	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:27.635762930 CET	192.168.2.4	8.8.8.8	0x9dbd	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:34.058247089 CET	192.168.2.4	8.8.8.8	0xe9e4	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:41.164343119 CET	192.168.2.4	8.8.8.8	0xb69e	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:46.980333090 CET	192.168.2.4	8.8.8.8	0x5e8e	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:53.068682909 CET	192.168.2.4	8.8.8.8	0xdf2c	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:00.094484091 CET	192.168.2.4	8.8.8.8	0xf2c9	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:06.075536013 CET	192.168.2.4	8.8.8.8	0x9fba	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:13.109258890 CET	192.168.2.4	8.8.8.8	0xceb4	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:18.079467058 CET	192.168.2.4	8.8.8.8	0x1ecc	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:25.099489927 CET	192.168.2.4	8.8.8.8	0xdec2	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:31.103212118 CET	192.168.2.4	8.8.8.8	0x2a85	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:37.087351084 CET	192.168.2.4	8.8.8.8	0x3011	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:44.087116957 CET	192.168.2.4	8.8.8.8	0x3d4d	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:51.129041910 CET	192.168.2.4	8.8.8.8	0x3699	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:57.229067087 CET	192.168.2.4	8.8.8.8	0x7f79	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:53:04.241309881 CET	192.168.2.4	8.8.8.8	0xa1	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 19, 2021 07:53:11.266027927 CET	192.168.2.4	8.8.8.8	0xfb68	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:53:17.334252119 CET	192.168.2.4	8.8.8.8	0x71eb	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:53:24.345340014 CET	192.168.2.4	8.8.8.8	0xad5	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)
Jan 19, 2021 07:53:29.325831890 CET	192.168.2.4	8.8.8.8	0x9360	Standard query (0)	cool.gotdns.ch	A (IP address)	IN (0x0001)

DNS Answers

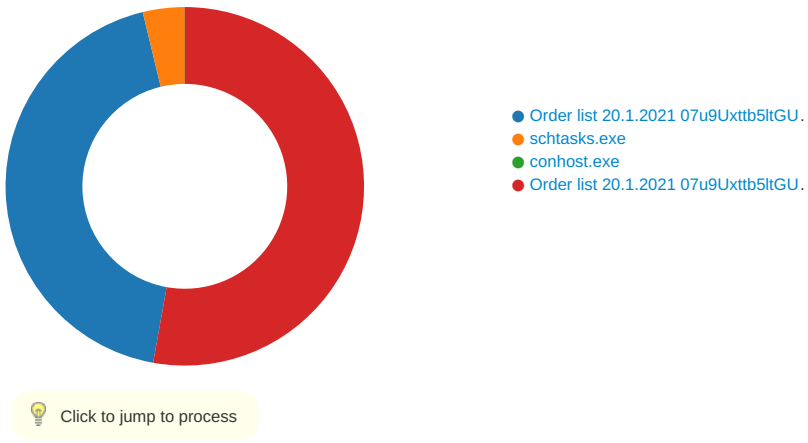
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 19, 2021 07:50:47.152731895 CET	8.8.8.8	192.168.2.4	0xdb52	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:50:54.034387112 CET	8.8.8.8	192.168.2.4	0x4dc3	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:01.195585012 CET	8.8.8.8	192.168.2.4	0x5504	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:07.135196924 CET	8.8.8.8	192.168.2.4	0xd323	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:13.584745884 CET	8.8.8.8	192.168.2.4	0x8d5a	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:20.406888962 CET	8.8.8.8	192.168.2.4	0xd67b	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:27.694797039 CET	8.8.8.8	192.168.2.4	0x9dbd	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:34.119842052 CET	8.8.8.8	192.168.2.4	0xe9e4	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:41.217613935 CET	8.8.8.8	192.168.2.4	0xb69e	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:47.039541960 CET	8.8.8.8	192.168.2.4	0x5e8e	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:51:53.127065897 CET	8.8.8.8	192.168.2.4	0xdf2c	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:00.155435085 CET	8.8.8.8	192.168.2.4	0xf2c9	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:06.131798983 CET	8.8.8.8	192.168.2.4	0x9fba	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:13.170758009 CET	8.8.8.8	192.168.2.4	0xceb4	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:18.135664940 CET	8.8.8.8	192.168.2.4	0x1ecc	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:25.155678034 CET	8.8.8.8	192.168.2.4	0xdec2	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:31.159454107 CET	8.8.8.8	192.168.2.4	0x2a85	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:37.149038076 CET	8.8.8.8	192.168.2.4	0x3011	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:44.143927097 CET	8.8.8.8	192.168.2.4	0x3d4d	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:51.177094936 CET	8.8.8.8	192.168.2.4	0x3699	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:52:57.288357973 CET	8.8.8.8	192.168.2.4	0x7f79	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:53:04.297863007 CET	8.8.8.8	192.168.2.4	0xa1	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 19, 2021 07:53:11.328566074 CET	8.8.8.8	192.168.2.4	0xfb68	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:53:17.392471075 CET	8.8.8.8	192.168.2.4	0x71eb	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:53:24.403909922 CET	8.8.8.8	192.168.2.4	0xad5	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)
Jan 19, 2021 07:53:29.384881020 CET	8.8.8.8	192.168.2.4	0x9360	No error (0)	cool.gotdns.ch		185.19.85.136	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Order list 20.1.2021 07u9Uxttb5ltGU.exe PID: 6148 Parent PID: 5932

General

Start time:	07:50:37
Start date:	19/01/2021
Path:	C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.exe'
Imagebase:	0xf0000
File size:	1741312 bytes
MD5 hash:	8935C408C5650172E350ACB92E7CC659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.662843036.000000000276B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.664198703.0000000003F65000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.664198703.0000000003F65000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.664198703.0000000003F65000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D38CF06	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	6D38CF06	unknown
C:\Users\user\AppData\Roaming\gIZSEI.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	6C1DDD66	CopyFileW
C:\Users\user\AppData\Roaming\gIZSEI.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C1DDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpE60F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C1D7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order list 20.1.2021 07u9Uxttb5ltGU.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE60F.tmp	success or wait	1	6C1D6A95	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\gIZSEI.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 a5 2a 06 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 be 18 00 00 d2 01 00 00 00 00 00 0e dd 18 00 00 20 00 00 00 e0 18 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 e0 1a 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....*.`.......... ....P................. ....@.. ....@................	success or wait	7	6C1DDD66	CopyFileW
C:\Users\user\AppData\Roaming\gIZSEI.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	6C1DDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpE60F.tmp	unknown	1639	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 6a 6f 6e 65 73 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 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6C1D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order list 20.1.2021 07u9Uxttb5ltGU.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D69C907	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Analysis Process: schtasks.exe PID: 6124 Parent PID: 6148

General

Start time:	07:50:41
Start date:	19/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\gIZSEI' /XML 'C:\Users\user\AppData\Local\Temp\tmpE60F.tmp'
Imagebase:	0xa40000
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\tmpE60F.tmp	unknown	2	success or wait	1	A4AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE60F.tmp	unknown	1640	success or wait	1	A4ABD9	ReadFile

Analysis Process: conhost.exe PID: 4612 Parent PID: 6124

General

Start time:	07:50:42
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Order list 20.1.2021 07u9Uxttb5ltGU.exe PID: 5040 Parent PID: 6148

General

Start time:	07:50:42
Start date:	19/01/2021
Path:	C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.exe
Imagebase:	0x6c0000
File size:	1741312 bytes
MD5 hash:	8935C408C5650172E350ACB92E7CC659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D38CF06	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	6D38CF06	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	6C1DBEFF	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	6C1D1E60	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	6C1DBEFF	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	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	20	6C1D1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.exe:Zone.Identifier	success or wait	1	5207C7E	DeleteFileA

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	a1 c1 cd 8b 46 bc d8 48	....F..H	success or wait	1	6C1D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	6	6C1D1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327432	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wp K .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_....Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6C1D1B4F	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.exe	unknown	4096	success or wait	1	6D34D72F	unknown
C:\Users\user\Desktop\Order list 20.1.2021 07u9Uxttb5ltGU.exe	unknown	512	success or wait	1	6D34D72F	unknown

Disassembly

Code Analysis