ID: 383611
Sample Name: AIC7VMxudf.exe
Cookbook: default.jbs
Time: 02:46:16
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

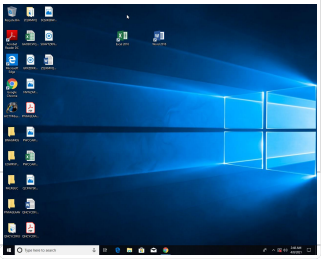
Analysis Report AIC7VMxudf.exe

Overview

General Information

Sample Name:	AIC7VMxudf.exe
Analysis ID:	383611
MD5:	d14d623ad514f6e.
SHA1:	d5a787167ab02d..
SHA256:	ff6ac9d2d223f20…
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

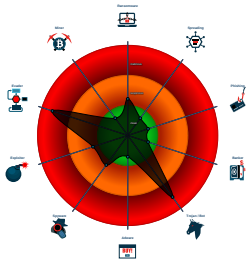
Nanocore

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

Signatures

- Detected Nanocore Rat
- 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…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains method …
- .NET source code contains potentia…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- AIC7VMxudf.exe (PID: 4872 cmdline: 'C:\Users\user\Desktop\AIC7VMxudf.exe' MD5: D14D623AD514F6EF05FB94541868B29C)
  - schtasks.exe (PID: 2044 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TqksXQmEOtil' /XML 'C:\Users\user\AppData\Local\Temp\tmp819D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4928 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6136 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
  - RegSvcs.exe (PID: 6100 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.203974120.0000000002C81000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.204528446.0000000003C89000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x4a6cd:$x1: NanoCore.ClientPluginHost • 0x281d7d:$x1: NanoCore.ClientPluginHost • 0x4a70a:$x2: IClientNetworkHost • 0x281dba:$x2: IClientNetworkHost • 0x4e23d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x2858ed:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.204528446.0000000003C89000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.204528446.0000000003C8 9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x4a435:$a: NanoCore • 0x4a445:$a: NanoCore • 0x4a679:$a: NanoCore • 0x4a68d:$a: NanoCore • 0x4a6cd:$a: NanoCore • 0x281ae5:$a: NanoCore • 0x281af5:$a: NanoCore • 0x281d29:$a: NanoCore • 0x281d3d:$a: NanoCore • 0x281d7d:$a: NanoCore • 0x4a494:$b: ClientPlugin • 0x4a696:$b: ClientPlugin • 0x4a6d6:$b: ClientPlugin • 0x281b44:$b: ClientPlugin • 0x281d46:$b: ClientPlugin • 0x281d86:$b: ClientPlugin • 0x4a5bb:$c: ProjectData • 0x281c6b:$c: ProjectData • 0x38c022:$c: ProjectData • 0x426a42:$c: ProjectData • 0x4afc2:$d: DESCrypto
Process Memory Space: AIC7VMxudf.exe PID: 4872	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x119f48:$x1: NanoCore.ClientPluginHost • 0x19898e:$x1: NanoCore.ClientPluginHost • 0x119fa9:$x2: IClientNetworkHost • 0x1989ef:$x2: IClientNetworkHost • 0x11f3ae:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x12d320:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcb w8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x19ddf4:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x1abd66:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcb w8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.AIC7VMxudf.exe.3efabf0.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.AIC7VMxudf.exe.3efabf0.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
0.2.AIC7VMxudf.exe.3efabf0.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.AIC7VMxudf.exe.3efabf0.4.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
0.2.AIC7VMxudf.exe.2c868c4.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 3 entries				

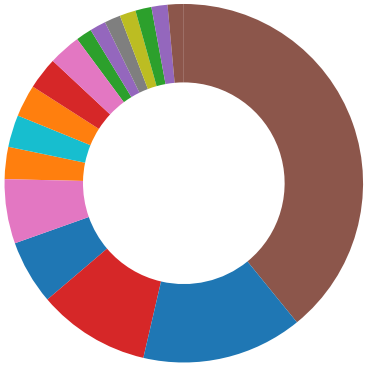
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- 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

Networking:

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains method to dynamically call methods (often used by packers)

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

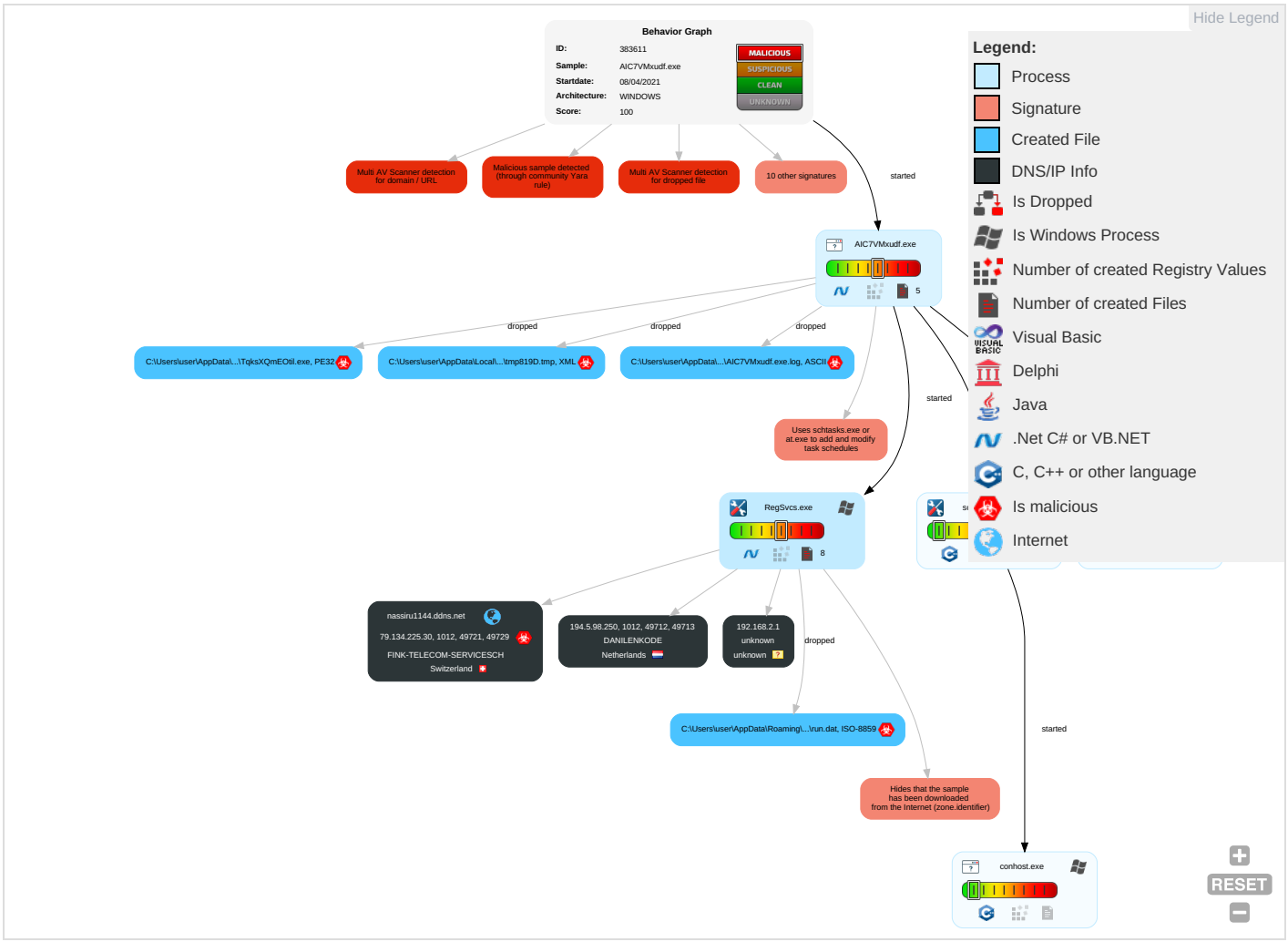
Detected Nanocore Rat

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
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access P

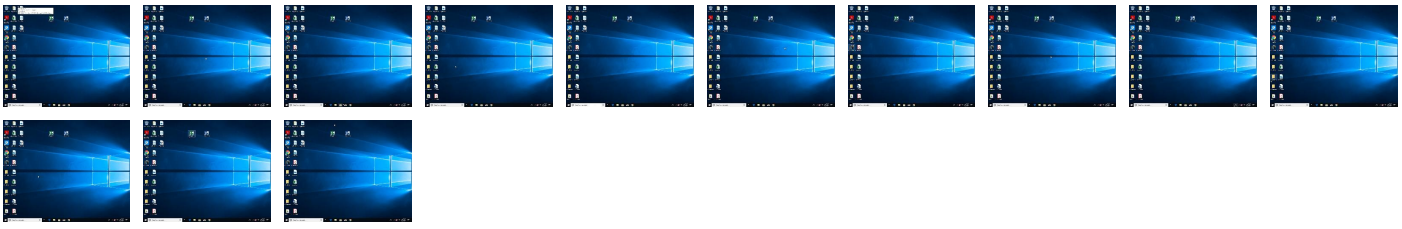
Behavior Graph



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
AIC7VMxudf.exe	51%	Virustotal		Browse
AIC7VMxudf.exe	32%	Metadefender		Browse
AIC7VMxudf.exe	69%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\TqksXQmEOtil.exe	51%	Virustotal		Browse
C:\Users\user\AppData\Roaming\TqksXQmEOtil.exe	32%	Metadefender		Browse
C:\Users\user\AppData\Roaming\TqksXQmEOtil.exe	69%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
nassiru1144.ddns.net	8%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nassiru1144.ddns.net	79.134.225.30	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	AIC7VMxudf.exe, 00000000.00000002.203974120.0000000002C81000.00000004.00000001.sdmp	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	AIC7VMxudf.exe, 00000000.00000002.203974120.0000000002C81000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.250	unknown	Netherlands		208476	DANILENKODE	false
79.134.225.30	nassiru1144.ddns.net	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383611
Start date:	08.04.2021
Start time:	02:46:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AIC7VMxudf.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:	27
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@8/7@16/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 61.2% • Quality standard deviation: 30.2%
HCA Information:	• Successful, ratio: 100% • 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): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 40.88.32.150, 52.147.198.201, 13.64.90.137, 52.255.188.83, 20.82.210.154, 23.54.113.104, 23.10.249.26, 23.10.249.43, 20.54.26.129, 20.82.209.183 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.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
02:47:02	API Interceptor	1x Sleep call for process: AIC7VMxudf.exe modified
02:47:06	API Interceptor	1054x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.98.250	IpEtbpwMpM.exe	Get hash	malicious	Browse	
	LOT 15 - Transfer Manifest.xlsx	Get hash	malicious	Browse	
	F8ZoCqWINT.exe	Get hash	malicious	Browse	
	xxRtA2mCLA.exe	Get hash	malicious	Browse	
	w6LWFElNpK.exe	Get hash	malicious	Browse	
	wxcV2YuXBj.exe	Get hash	malicious	Browse	
	Ref 19117030.xlsx	Get hash	malicious	Browse	
	PO_SRL2020426.xlsx	Get hash	malicious	Browse	
	FztmRe1Bcb.exe	Get hash	malicious	Browse	
79.134.225.30	Payment Confirmation.exe	Get hash	malicious	Browse	
	JOIN.exe	Get hash	malicious	Browse	
	Itinerary.pdf.exe	Get hash	malicious	Browse	
	vVH0wIFYFd.exe	Get hash	malicious	Browse	
	GWee9QSphp.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	s7pnYY2USl.jar	Get hash	malicious	Browse	
	s7pnYY2USl.jar	Get hash	malicious	Browse	
	SecuriteInfo.com.BehavesLike.Win32.Generic.dc.exe	Get hash	malicious	Browse	
	Import and Export Regulation.xlsx	Get hash	malicious	Browse	
	BBdzKOGQ36.exe	Get hash	malicious	Browse	
	BL.exe	Get hash	malicious	Browse	
	Payment Invoice.exe	Get hash	malicious	Browse	
	Payment Invoice.pdf.exe	Get hash	malicious	Browse	
	Inquiries_scan_011023783591374376585.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	n4CeZTejKM.exe	Get hash	malicious	Browse	• 194.5.98.9
	New Order request Ref E100-#3175704534,pdf.e.exe	Get hash	malicious	Browse	• 194.5.97.14
	PO-#3175704534,PDF.exe	Get hash	malicious	Browse	• 194.5.97.14
	Evgp2DqQha.exe	Get hash	malicious	Browse	• 194.5.98.107
	Payment Copy #6578965432.exe	Get hash	malicious	Browse	• 194.5.98.52
	PO SKP 149684.jar	Get hash	malicious	Browse	• 194.5.98.48
	4EPXPkicIL.exe	Get hash	malicious	Browse	• 194.5.97.158
	xoxd454e9q.exe	Get hash	malicious	Browse	• 194.5.97.158
	1VzQLgPeAlfHSHQ.exe	Get hash	malicious	Browse	• 194.5.97.214
	XJ1lVmdiCi.exe	Get hash	malicious	Browse	• 194.5.97.237
	QUOTATIONs#280321_RFQ_PRODUCTS_ENQUIRY_TRINITY_VIETNAM_CO.exe	Get hash	malicious	Browse	• 194.5.98.182
	Revised invoice30032021.exe	Get hash	malicious	Browse	• 194.5.98.145
	QUOTATIONs#280321_RFQ_PRODUCTS_ENQUIRY_TRINITY_VIETNAM_CO.exe	Get hash	malicious	Browse	• 194.5.98.182
	Vp0VO1U2oo.exe	Get hash	malicious	Browse	• 194.5.98.107
	IpEtbpwMpM.exe	Get hash	malicious	Browse	• 194.5.98.250
	LOT 15 - Transfer Manifest.xlsx	Get hash	malicious	Browse	• 194.5.98.250
	2df27f1a3505dbd0995188d49c253f5bc53c0e994954c.exe	Get hash	malicious	Browse	• 194.5.98.107
	1AQz4ua1TU.exe	Get hash	malicious	Browse	• 194.5.98.107
	5YjMB4pzS4.exe	Get hash	malicious	Browse	• 194.5.98.49
	F8ZoCqWINT.exe	Get hash	malicious	Browse	• 194.5.98.250
FINK-TELECOM-SERVICESCH	9mm case for ROYAL METAL INDUSTRIES 3milmonth Specification drawings.exe	Get hash	malicious	Browse	• 79.134.225.21
	PO50164.exe	Get hash	malicious	Browse	• 79.134.225.79
	Fast color scan to a PDFfile_1_20210331084231346.pdf.exe	Get hash	malicious	Browse	• 79.134.225.102
	n7dIHuG3v6.exe	Get hash	malicious	Browse	• 79.134.225.92
	F6JT4fXIAQ.exe	Get hash	malicious	Browse	• 79.134.225.92
	order_inquiry2094.xls.exe	Get hash	malicious	Browse	• 79.134.225.102
	5H957qLghX.exe	Get hash	malicious	Browse	• 79.134.225.25
	yBio5dWAOl.exe	Get hash	malicious	Browse	• 79.134.225.7
	wDIaJji4Vv.exe	Get hash	malicious	Browse	• 79.134.225.7
	DkZY1k3y9F.exe	Get hash	malicious	Browse	• 79.134.225.23
	hbvo9thTAX.exe	Get hash	malicious	Browse	• 79.134.225.7
	SCAN ORDER DOC 040202021.exe	Get hash	malicious	Browse	• 79.134.225.71
	Waybill Doc_pdf.exe	Get hash	malicious	Browse	• 79.134.225.92
	gfcYixSdyD.exe	Get hash	malicious	Browse	• 79.134.225.71
	cJtVGjtNGZ.exe	Get hash	malicious	Browse	• 79.134.225.40
	Transferwise beneficiary detailspdf.exe	Get hash	malicious	Browse	• 79.134.225.22
	NS 001 DOP IPS ORIENTATIONS.doc	Get hash	malicious	Browse	• 79.134.225.73
	cp.msi.exe	Get hash	malicious	Browse	• 79.134.225.109
	ot.msi	Get hash	malicious	Browse	• 79.134.225.109
	dd.exe	Get hash	malicious	Browse	• 79.134.225.109

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AIC7VMxudf.exe.log	
Process:	C:\Users\user\Desktop\AIC7VMxudf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	706
Entropy (8bit):	5.342604339328228
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCqDLI4MWuPk21q1KDLI4Mq92n4M9XKbbDLI4MWuPJKiUrRt:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3Vt
MD5:	5DDFC467AB8C44DEA19603E0ECDA810D
SHA1:	BE369FE7C7D3A4D32886C1BA7319FCA14BA40776
SHA-256:	AE759C8FFA5038FC35A1F3C27EC1401909248A05E207CD940CBEF821E02B5A59
SHA-512:	A242206D3D83E5242E09F82677C4C4D9A9E400354607B8F749195E8BE383EA1F31DE62D5123C5197BE78812856955772D6302588A104BB16A0977713A155439E
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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..

C:\Users\user\AppData\Local\Temp\tmp819D.tmp	
Process:	C:\Users\user\Desktop\AIC7VMxudf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.193797103861353
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBrBtn:cbh47TlNQ//rydbz9l3YODOLNdq3V
MD5:	80385303CD5BBCE7CD306E0FF332C35E
SHA1:	5E8C4EFC88C2264B00BE4D82F84D8D71A7AB7EB3
SHA-256:	4B279EFC48FB03FD795202AD7753334967CA327D611CC0E04B569EFE3C30101A
SHA-512:	A6E9A8B7E3AFF34D2ECFE1794E4B2D677427288A57D5D1B6832ECE9697AA17397E38D061E01A74FF5B7B6E00A947D7B3A82D188730DD1DD611AE074E0FD9AAA
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:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	864
Entropy (8bit):	7.012278113302776
Encrypted:	false
SSDEEP:	24:IQnybgCyHJ5lQnybgCyHJ5lQnybgCyHJ5lQnybgCyHJ5i:IkR5lkR5lkR5lkR5i
MD5:	281F575A1418DE9976BA07B4A58F860B
SHA1:	275A3E5F9E5064B8DE30E3AC1C089109C2FE22D6
SHA-256:	3736A2E2E6F777CACC098F9B7F7B5770A045B4952AEC6182448E730D116A0B5B
SHA-512:	ED86C8051D8F47DA5DD1C6AA637278CA014E9DBB0AEE5B3D194446F38B5C411DE37AF5A909998AFE930326A7A4CF4632BCAE85E5AC6D145E2E9EC784F64B95D6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S.5.6.C4..E.Y.|.....).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1.....r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S.5.6.C4..E.Y.|.....).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1.....r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S.5.6.C4..E.Y.|.....).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1.....r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL|X

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ISO-8859 text
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:GP:W
MD5:	BCF72E34F695DA2FE3C6859FB39A68CF
SHA1:	5CC167E48BC3C14D9FCF8A9DBB906FAE3554BCF4
SHA-256:	DB15F8F0FDFB3CAF164B7EE5114BFA58E21F1012CE187B093C6316BF1F0D6565
SHA-512:	F0985CC1CE4BF8DBECF6DC4019C69AB9D2BCE3B50451DD2A03759BB8C00365576FABFC7E3B6847AF191E4898B317309B80A741BE863DAD3B84419829B672AB9
Malicious:	**true**
Reputation:	low
Preview:	7..Es..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	327928
Entropy (8bit):	**7.999564270615327**
Encrypted:	**true**
SSDEEP:	6144:EV615kOliaxupZQLNJLtpAUVmDkva49avhcpi4sXZCKnQhi2dDBSjYh:4615HtupZQLNJLvAdDkxDgXePph
MD5:	78E439043BA0679B60222A2ADF210FA6
SHA1:	3321C991EB442CD04F8AE4AC446FFD3A0EC2F693
SHA-256:	B39C660B6B9393FE0DA45B730B6BFA7C7780A20EB196890F57500D9F91E76408
SHA-512:	82E4B6765204E7A33CF7BED5B261BA658043E6343FFBFD0FEF29883377D1EE8CAA64B60D48C281B4598FB01D1146EFEA5DCECB4A41BE0B25DDA013AD263B221B
Malicious:	false
Reputation:	low
Preview:	..,!..LJy..5<...9....!..?.AJ.._!..Px.9g..._t...].....t../...a.k.Z3.H...o..>.6.x.E.....hBu*.#.Z..v..).#..x...hl..e...B-<.J0...o...]....%.....51.h..G{.u.|*r..xs.d..#....).&.e.3..6.V+....d.....!..v...)Y.....pe...c.mW.....O.X...>.[.....w^.0.&Z.^5se.(..1 Zq.....G.`y.F.f..T[k.^.fj.o.~...t.=..[...zU8_..b...%.....J.6._..._!{.c... .8...^.....^..|...7T.c.._X/n..Fd.M>.=..Cmwd.%N.S.-..jk!.B.q>S...7.h....?sa.S@..3...G.B.M..Q.f..b....j..0y.i&..$...LIq}&..8F.....m.....=..5O.g...}"4.....z.q.b.Am.A1."]"".....C..F..9.2.u.DL..s.=^.s.@..k.c>.u...rw.W.E....Jn.....$...C...0../.I.M...D._.K.d.2...|...T....1.....g.-x.....U$.I.n...e..|J...AVU.v.I..3.7%&.6.....)....@f.....}TR...g]W8x..."...{.H.....gS,..@.).....L...K7.'V.42...~.b..q.j.V.1...V..`.NW*].l6A...c.<..5..'..u...i...*...L..'..!.cD..m...3~....As.@+....'&..\4_...6..t.jq2IK.K.2..E&.K..wi9...enm.7...0.EVG.Ab....S...(%.of.b.?.J..;."0....0u.%.M....(a...A.LEn....P.z.x.3.8....G.....MT.:

C:\Users\user\AppData\Roaming\TqksXQmEOtil.exe	
Process:	C:\Users\user\Desktop\AIC7VMxudf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1182208
Entropy (8bit):	7.2992351228535135
Encrypted:	false
SSDEEP:	12288:phwL5gPTbbOgk79rgPe0Fe2AltwWyT1oJbwkMhRouR1+xsvqdEPKyBKpBr/LTn:p9I7fGXWyxoE6uREsvqCdK7T
MD5:	D14D623AD514F6EF05FB94541868B29C
SHA1:	D5A787167AB02D7FD194FCCB1F6335C8927702AD
SHA-256:	FF6AC9D2D223F204F998EB31CF4DC2045BEE3BA86F481D8CEA7A8B24A2EBF889
SHA-512:	44D7E0CA90A31BA45378445AF292D1E3DA2EDC7FB2B774BBB35D519E33DA5DA20E3D4A9253BC8916B8D7AFA94EB16974B899C0927BE45941EAC8167D3943982
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 51%, Browse • Antivirus: Metadefender, Detection: 32%, Browse • Antivirus: ReversingLabs, Detection: 69%
Reputation:	low

C:\Users\user\AppData\Roaming\TqksXQmEOtil.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....``.....P.....L....."..... .....@.. .....`..... ..@.....O.....H.....@..... ..... ..H.....text...(.... ..... ..`.rsrc....H.....J.....@..@.rel oc.....@.....@..B.....H.....(....*&..(....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0..... .....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*&..()....*...0..<.....~.....(*.....,!r...p.....(+...o,...s-.....~.....+..*.0.....~.....+..*".....*.0..... (....r...p~....o.....+..*...0..<.....~.....(*.....,!r7..p.....(+

C:\Users\user\AppData\Roaming\TqksXQmEOtil.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\AIC7VMxudf.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):	7.2992351228535135
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	AIC7VMxudf.exe
File size:	1182208
MD5:	d14d623ad514f6ef05fb94541868b29c
SHA1:	d5a787167ab02d7fd194fccb1f6335c8927702ad
SHA256:	ff6ac9d2d223f204f998eb31cf4dc2045bee3ba86f481d8cea7a8b24a2ebf889
SHA512:	44d7e0ca90a31ba45378445af292d1e3da2edc7fb2b774bbb35d519e33da5da20e3d4a9253bc8916b8d7afa94eb16974b899c0927be45941eac8167d39439812
SSDEEP:	12288:phwL5gPTbbOgk79rgPe0Fe2AltwWyT1oJbwkMhRouR1+xsvqdEPKyBKpBr/LTn:p9l7fGXWyxoE6uREsvqCdK7T
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....``.....P.....L....."..... .....@.. .....`.....@.....

File Icon

Icon Hash:	e9e8d8943a9df936

Static PE Info

General

Entrypoint:	0x51db22
Entrypoint Section:	.text
Digitally signed:	false

General

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:	0x6060F7AD [Sun Mar 28 21:39:57 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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	0x11dad0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x11e000	0x48d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x124000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x11bb28	0x11bc00	False	0.655929928414	data	7.31668862644	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x11e000	0x48d8	0x4a00	False	0.552892736486	data	5.25809431394	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x124000	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	0x11e100	0x4228	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0x122338	0x14	data		
RT_VERSION	0x12235c	0x37c	data		
RT_MANIFEST	0x1226e8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

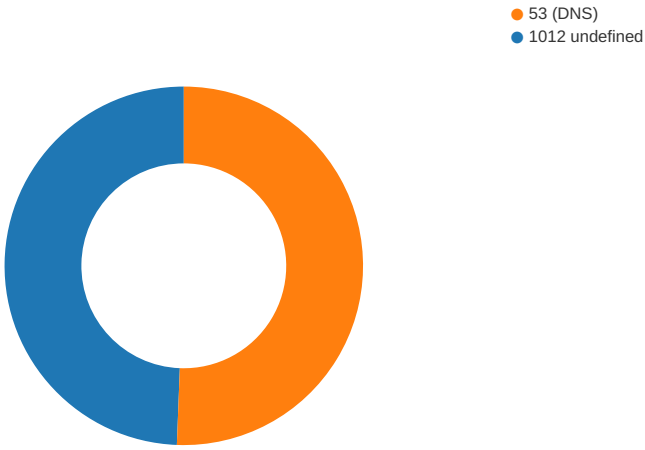
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2021 Handy Dan
Assembly Version	1.1.0.0
InternalName	IMoniker.exe
FileVersion	1.1.0.0
CompanyName	Handy Dan
LegalTrademarks	
Comments	2002 Honda S-MX
ProductName	PassengerService
ProductVersion	1.1.0.0
FileDescription	PassengerService
OriginalFilename	IMoniker.exe

Network Behavior

Network Port Distribution

Total Packets: 81



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 02:47:06.840564013 CEST	49712	1012	192.168.2.3	194.5.98.250
Apr 8, 2021 02:47:06.878880024 CEST	1012	49712	194.5.98.250	192.168.2.3
Apr 8, 2021 02:47:07.383434057 CEST	49712	1012	192.168.2.3	194.5.98.250
Apr 8, 2021 02:47:07.422149897 CEST	1012	49712	194.5.98.250	192.168.2.3
Apr 8, 2021 02:47:07.930614948 CEST	49712	1012	192.168.2.3	194.5.98.250
Apr 8, 2021 02:47:07.968980074 CEST	1012	49712	194.5.98.250	192.168.2.3
Apr 8, 2021 02:47:12.025633097 CEST	49713	1012	192.168.2.3	194.5.98.250
Apr 8, 2021 02:47:12.063585043 CEST	1012	49713	194.5.98.250	192.168.2.3
Apr 8, 2021 02:47:12.571551085 CEST	49713	1012	192.168.2.3	194.5.98.250
Apr 8, 2021 02:47:12.610152006 CEST	1012	49713	194.5.98.250	192.168.2.3
Apr 8, 2021 02:47:13.118459940 CEST	49713	1012	192.168.2.3	194.5.98.250
Apr 8, 2021 02:47:13.156709909 CEST	1012	49713	194.5.98.250	192.168.2.3
Apr 8, 2021 02:47:17.167402029 CEST	49716	1012	192.168.2.3	194.5.98.250
Apr 8, 2021 02:47:17.205554962 CEST	1012	49716	194.5.98.250	192.168.2.3
Apr 8, 2021 02:47:17.712423086 CEST	49716	1012	192.168.2.3	194.5.98.250
Apr 8, 2021 02:47:17.750607014 CEST	1012	49716	194.5.98.250	192.168.2.3
Apr 8, 2021 02:47:18.259725094 CEST	49716	1012	192.168.2.3	194.5.98.250
Apr 8, 2021 02:47:18.298007965 CEST	1012	49716	194.5.98.250	192.168.2.3
Apr 8, 2021 02:47:22.396223068 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:22.598064899 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:22.598198891 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:22.626696110 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:22.856774092 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:22.956831932 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:23.009783983 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:23.042960882 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:23.295963049 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:23.296076059 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:23.570842981 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:23.570974112 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:23.853091955 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:23.886234999 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:23.886564970 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:23.886658907 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:23.889122963 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:23.895214081 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:23.895253897 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:23.895286083 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:23.895323038 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:23.895350933 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:23.895386934 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:23.895385981 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:23.895411015 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:23.895415068 CEST	49721	1012	192.168.2.3	79.134.225.30

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 02:47:23.895420074 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:23.895683050 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.104693890 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.109807014 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.109949112 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.110122919 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.111001015 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.111042976 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.111119032 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.112234116 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.112283945 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.112365007 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.112382889 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.112603903 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.112859964 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.118292093 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.118467093 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.118573904 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.118654966 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.118724108 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.118727922 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.118787050 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.120322943 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.120486021 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.120570898 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.120872021 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.121140003 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.121218920 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.121402025 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.121541977 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.121588945 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.121615887 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.121639013 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.122600079 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.124032021 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.316298008 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.316354036 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.316549063 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.317137957 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.317416906 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.317558050 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.317684889 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.317914009 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.318003893 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.318749905 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.318790913 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.318892002 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.319561958 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.324621916 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.325728893 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.325773001 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.325896978 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.327254057 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.327672005 CEST	1012	49721	79.134.225.30	192.168.2.3
Apr 8, 2021 02:47:24.327821016 CEST	49721	1012	192.168.2.3	79.134.225.30
Apr 8, 2021 02:47:24.328212023 CEST	1012	49721	79.134.225.30	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 02:46:53.952297926 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:46:53.966980934 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 8, 2021 02:46:54.760468960 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:46:54.774353027 CEST	53	55984	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 02:46:55.433089018 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:46:55.446239948 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 8, 2021 02:46:56.102468967 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:46:56.116492987 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 02:46:57.156429052 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:46:57.170727968 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 8, 2021 02:46:58.091542959 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:46:58.105937004 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:14.745675087 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:14.758429050 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:16.099215984 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:16.111876011 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:17.561136007 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:17.573775053 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:18.882030964 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:18.894682884 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:19.534041882 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:19.546690941 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:21.730972052 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:21.744327068 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:22.374803066 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:22.388505936 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:22.394206047 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:22.400437117 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:23.286155939 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:23.300271034 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:24.607961893 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:24.620454073 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:25.267237902 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:25.279891968 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:26.050910950 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:26.090246916 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:28.152350903 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:28.165757895 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:29.144176960 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:29.163738966 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:33.189938068 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:33.245075941 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:35.207701921 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:35.221071959 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:38.098249912 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:38.116609097 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:42.209163904 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:42.221930027 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:48.389548063 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:48.402282953 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:51.611351013 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:51.626709938 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 8, 2021 02:47:54.659351110 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:47:54.679435968 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 8, 2021 02:48:01.586961985 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:48:01.599728107 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 8, 2021 02:48:04.910753012 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:48:04.923286915 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 8, 2021 02:48:08.500825882 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:48:08.514415979 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 02:48:08.553947926 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:48:08.567161083 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 8, 2021 02:48:14.635277033 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:48:14.648689032 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 02:48:20.674544096 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:48:20.694863081 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 8, 2021 02:48:27.741358042 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:48:27.754797935 CEST	53	56130	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 02:48:34.736381054 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:48:34.835853100 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 8, 2021 02:48:40.013205051 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:48:40.025350094 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 8, 2021 02:48:41.896703005 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:48:41.931121111 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 8, 2021 02:48:42.371321917 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:48:42.390798092 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 8, 2021 02:48:49.369277000 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:48:49.382922888 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 8, 2021 02:48:56.355611086 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:48:56.369214058 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 8, 2021 02:49:03.066452980 CEST	56803	53	192.168.2.3	8.8.8.8
Apr 8, 2021 02:49:03.080234051 CEST	53	56803	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 02:47:22.374803066 CEST	192.168.2.3	8.8.8.8	0x421b	Standard query (0)	nassiru1144.ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 02:47:29.144176960 CEST	192.168.2.3	8.8.8.8	0x225f	Standard query (0)	nassiru1144.ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 02:47:35.207701921 CEST	192.168.2.3	8.8.8.8	0xd91c	Standard query (0)	nassiru1144.ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 02:47:42.209163904 CEST	192.168.2.3	8.8.8.8	0x1511	Standard query (0)	nassiru1144.ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 02:47:48.389548063 CEST	192.168.2.3	8.8.8.8	0x509f	Standard query (0)	nassiru1144.ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 02:47:54.659351110 CEST	192.168.2.3	8.8.8.8	0x214e	Standard query (0)	nassiru1144.ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:01.586961985 CEST	192.168.2.3	8.8.8.8	0x485d	Standard query (0)	nassiru1144.ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:08.553947926 CEST	192.168.2.3	8.8.8.8	0x927d	Standard query (0)	nassiru1144.ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:14.635277033 CEST	192.168.2.3	8.8.8.8	0x1542	Standard query (0)	nassiru1144.ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:20.674544096 CEST	192.168.2.3	8.8.8.8	0x18e1	Standard query (0)	nassiru1144.ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:27.741358042 CEST	192.168.2.3	8.8.8.8	0x8571	Standard query (0)	nassiru1144.ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:34.736381054 CEST	192.168.2.3	8.8.8.8	0xb8b1	Standard query (0)	nassiru1144.ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:42.371321917 CEST	192.168.2.3	8.8.8.8	0xb51c	Standard query (0)	nassiru1144.ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:49.369277000 CEST	192.168.2.3	8.8.8.8	0x233b	Standard query (0)	nassiru1144.ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:56.355611086 CEST	192.168.2.3	8.8.8.8	0x95f1	Standard query (0)	nassiru1144.ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 02:49:03.066452980 CEST	192.168.2.3	8.8.8.8	0x3db4	Standard query (0)	nassiru1144.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

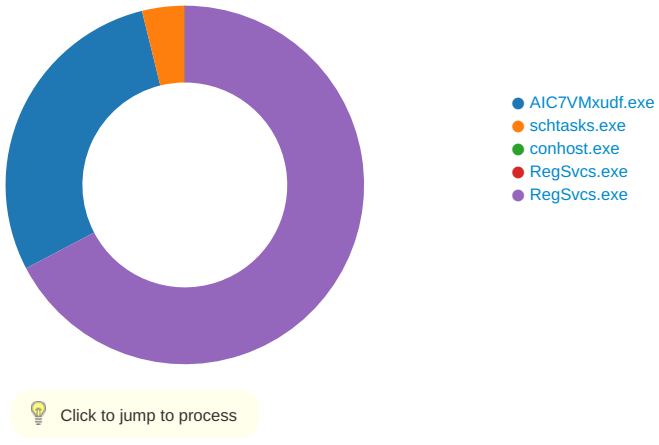
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 02:47:22.394206047 CEST	8.8.8.8	192.168.2.3	0x421b	No error (0)	nassiru1144.ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Apr 8, 2021 02:47:29.163738966 CEST	8.8.8.8	192.168.2.3	0x225f	No error (0)	nassiru1144.ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Apr 8, 2021 02:47:35.221071959 CEST	8.8.8.8	192.168.2.3	0xd91c	No error (0)	nassiru1144.ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Apr 8, 2021 02:47:42.221930027 CEST	8.8.8.8	192.168.2.3	0x1511	No error (0)	nassiru1144.ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Apr 8, 2021 02:47:48.402282953 CEST	8.8.8.8	192.168.2.3	0x509f	No error (0)	nassiru1144.ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Apr 8, 2021 02:47:54.679435968 CEST	8.8.8.8	192.168.2.3	0x214e	No error (0)	nassiru1144.ddns.net		79.134.225.30	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 02:48:01.599728107 CEST	8.8.8.8	192.168.2.3	0x485d	No error (0)	nassiru1144.ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:08.567161083 CEST	8.8.8.8	192.168.2.3	0x927d	No error (0)	nassiru1144.ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:14.648689032 CEST	8.8.8.8	192.168.2.3	0x1542	No error (0)	nassiru1144.ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:20.694863081 CEST	8.8.8.8	192.168.2.3	0x18e1	No error (0)	nassiru1144.ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:27.754797935 CEST	8.8.8.8	192.168.2.3	0x8571	No error (0)	nassiru1144.ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:34.835853100 CEST	8.8.8.8	192.168.2.3	0xb8b1	No error (0)	nassiru1144.ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:42.390798092 CEST	8.8.8.8	192.168.2.3	0xb51c	No error (0)	nassiru1144.ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:49.382922888 CEST	8.8.8.8	192.168.2.3	0x233b	No error (0)	nassiru1144.ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Apr 8, 2021 02:48:56.369214058 CEST	8.8.8.8	192.168.2.3	0x95f1	No error (0)	nassiru1144.ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Apr 8, 2021 02:49:03.080234051 CEST	8.8.8.8	192.168.2.3	0x3db4	No error (0)	nassiru1144.ddns.net		79.134.225.30	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AIC7VMxudf.exe PID: 4872 Parent PID: 5648

General

Start time:	02:47:00
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\AIC7VMxudf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\AIC7VMxudf.exe'
Imagebase:	0x690000
File size:	1182208 bytes
MD5 hash:	D14D623AD514F6EF05FB94541868B29C
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: 00000000.00000002.203974120.0000000002C81000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.204528446.0000000003C89000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.204528446.0000000003C89000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.204528446.0000000003C89000.00000004.00000001.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\AppData\Roaming\TqksXQmEOtil.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	6CF1DD66	CopyFileW
C:\Users\user\AppData\Roaming\TqksXQmEOtil.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CF1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp819D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF17038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AIC7VMxudf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp819D.tmp	success or wait	1	6CF16A95	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\TqksXQmEOtil.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 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 ad f7 60 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 bc 11 00 00 4c 00 00 00 00 00 00 22 db 11 00 00 20 00 00 00 e0 11 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 60 12 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......L......".... ....@.. ....` ....@.................	success or wait	5	6CF1DD66	CopyFileW
C:\Users\user\AppData\Roaming\ TqksXQmEOtil.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	6CF1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp819D.tmp	unknown	1645	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 68 61 72 64 7a 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.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationIn	success or wait	1	6CF11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AIC7VMxudf.exe.log	unknown	706	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 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 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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_v4.0.3	success or wait	1	6E3DC907	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	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile

Analysis Process: schtasks.exe PID: 2044 Parent PID: 4872

General

Start time:	02:47:03
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TqksXQmEOtil' /XML 'C:\Users\user\AppData\Local\Temp\tmp819D.tmp'
Imagebase:	0xad0000
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\tmp819D.tmp	unknown	2	success or wait	1	ADAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp819D.tmp	unknown	1646	success or wait	1	ADABD9	ReadFile

Analysis Process: conhost.exe PID: 4928 Parent PID: 2044

General

Start time:	02:47:03
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: RegSvcs.exe PID: 6136 Parent PID: 4872

General

Start time:	02:47:04
Start date:	08/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x350000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 6100 Parent PID: 4872

General

Start time:	02:47:04
Start date:	08/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x450000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0CCF06	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	6E0CCF06	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	6CF1BEFF	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	6CF11E60	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	6CF1BEFF	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	6CF1BEFF	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	14	6CF11E60	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	6CF11E60	CreateFileW

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	37 a0 0a 45 73 fa d8 48	7..Es..H	success or wait	1	6CF11B4F	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	216	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 50 f4 76 59 a1 02 b3 8b 02 19 e1 11 b5 53 f0 35 8a 36 12 43 34 2e dd 45 b1 59 db 7c f7 f1 8d 15 ba ff 7f 82 16 29 8e 7a 73 0c a9 ef 77 e2 b4 67 6c ef e7 5c ec 47 c3 1a 4a 18 4d f2 76 45 53 8c 30 e0 df 9b ff d2 9b 50 f7 3a 82 b9 36 fc f0 01 54 a7 89 a5 c8 2b 35 80 31 a7 c4 19 c1 b3 0c ea a6 a9 b1 9d e7 e0 c5 72 06 50 1d 56 9b 95 2b 91 e6 28 cc 2a 32 64 09 66 87 b6 cf 20 ed ed ba 9e 71 c3 85 cb 20 37 69 4f ca 2b 81 bb 63 da e6 8b b2 fa cf 09 21 c9 27 ed 2a c7 14 6d 4c 7c 58	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h.P.v Y.....S.5.6.C4..E.Y.|..... ....).zs...w..gl..\.G..J.M.vES .0.....P.:..6...T....+5.1.... .....r.P.V..+..(.*2d.f... ....q... 7iO.+..c.....!.'.* ..mL|X	success or wait	4	6CF11B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327928	99 84 2c 21 89 d0 bc 4c 4a 79 a3 fb 35 3c d3 01 96 39 95 b4 cf da 21 9e 1d 3f e3 bf bf 41 4a e9 14 5f 6c 90 ab 50 78 cb 39 67 f4 f6 d4 5f 74 a9 fa 03 5d dd 0c 0b e4 ce 74 fe ce 2f c4 f4 1b 61 be 6b b6 5a 33 c5 48 a7 f2 88 df 6f f9 0f 3e c2 36 8b 78 fc 45 02 8e 8c 8c be 68 42 75 2a 10 23 e3 be ac 5a 0a a1 76 be b7 29 cf 8d 23 cd f1 78 10 e0 c1 68 49 8d 12 65 fd cc eb 42 2d 3c 11 4a 30 f6 d1 d9 ae 6f 12 06 e3 b1 5d 92 cd c8 fb 25 a6 a5 e5 c7 8c be a7 35 31 eb 68 d1 d7 91 47 7b b2 75 16 7c 2a 72 10 a5 78 73 b8 64 8f e6 23 d9 cb db 9d d0 29 df ba 26 fd 65 9d 33 2e 80 36 ae 56 2b 8e b4 0a e0 64 b9 b6 d3 07 e7 ab 00 21 d5 c5 8a 76 8b 91 b0 29 59 ea 0e 83 9d 96 7f 70 65 95 e8 c6 b0 63 03 6d 57 8d 8f d4 cb de 4f e4 58 b1 9a b2 3e 1f 5b cb c7 c9 0d cc f6 77 5e d6	..,!...LJy..5<...9....!..?...A J.._I..Px.9g..._t...].....t../ ...a.k.Z3.H....o..>.6.x.E..... hBu*.#...Z..v..)..#..x...hI..e ...B-<.J0....o....]....%..... .51.h...G{.u.|*r..xs.d..#.....)..&.e.3..6.V+....d.....!... v...)Y.....pe....c.mW.....O.X ...>.[.....w^.	success or wait	1	6CF11B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E0ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	4096	success or wait	1	6E08D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	512	success or wait	1	6E08D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0 .0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6E08D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0 .0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6E08D72F	unknown

Disassembly

Code Analysis