

ID: 499570
Sample Name: Peixoto - QUOTATION LIST.exe
Cookbook: default.jbs
Time: 16:08:18
Date: 08/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report Peixoto - QUOTATION LIST.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 6
AV Detection: 6
E-Banking Fraud: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Jbx Signature Overview 6
AV Detection: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 7
Data Obfuscation: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 14
General 14
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 15
Data Directories 15
Sections 15
Resources 15
Imports 16
Version Infos 16
Network Behavior 16
Snort IDS Alerts 16
Network Port Distribution 16
TCP Packets 16
Code Manipulations 16
Statistics 16
Behavior 16

Copyright Joe Security LLC 2021

System Behavior 16
Analysis Process: Peixoto - QUOTATION LIST.exe PID: 5460 Parent PID: 5540 16
General 17
File Activities 17
File Created 17
File Written 17
File Read 17
Registry Activities 17
Key Value Modified 17
Analysis Process: Peixoto - QUOTATION LIST.exe PID: 6572 Parent PID: 5460 17
General 17
Analysis Process: Peixoto - QUOTATION LIST.exe PID: 6584 Parent PID: 5460 18
General 18
File Activities 19
File Created 19
File Deleted 19
File Written 19
File Read 19
Disassembly 19
Code Analysis 19

Copyright Joe Security LLC 2021

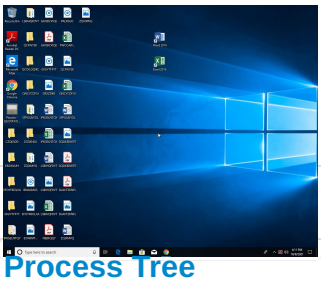
Windows Analysis Report Peixoto - QUOTATION LIST.exe

Overview

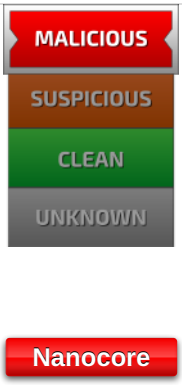
General Information

Sample Name:	Peixoto - QUOTATION LIST.exe
Analysis ID:	499570
MD5:	0f129aa97048f7e..
SHA1:	b597185c94fac60..
SHA256:	fcf3b27fdc54c53…
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection

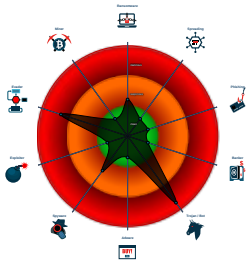


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- Peixoto - QUOTATION LIST.exe (PID: 5460 cmdline: 'C:\Users\user\Desktop\Peixoto - QUOTATION LIST.exe' MD5: 0F129AA97048F7EC0557B211349A2CE0)
  - Peixoto - QUOTATION LIST.exe (PID: 6572 cmdline: C:\Users\user\AppData\Local\Temp\Peixoto - QUOTATION LIST.exe MD5: 0F129AA97048F7EC0557B211349A2CE0)
  - Peixoto - QUOTATION LIST.exe (PID: 6584 cmdline: C:\Users\user\AppData\Local\Temp\Peixoto - QUOTATION LIST.exe MD5: 0F129AA97048F7EC0557B211349A2CE0)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "28a7a9fa-8b88-4ff1-be22-9ecea4e9",
  "Group": "T-C",
  "Domain1": "185.222.57.149",
  "Domain2": "127.0.0.1",
  "Port": 4557,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.507935886.000000000720 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x59eb:$x1: NanoCore.ClientPluginHost • 0x5b48:$x2: IClientNetworkHost
00000010.00000002.507935886.000000000720 0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x59eb:$x2: NanoCore.ClientPluginHost • 0x6941:$s3: PipeExists • 0x5be1:$s4: PipeCreated • 0x5a05:$s5: IClientLoggingHost
00000000.00000002.331468267.000000000352 B000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x37de5:$x1: NanoCore.ClientPluginHost • 0x5fe05:$x1: NanoCore.ClientPluginHost • 0x37e22:$x2: IClientNetworkHost • 0x5fe42:$x2: IClientNetworkHost • 0x3b955:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x63975:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.331468267.000000000352 B000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.331468267.000000000352 B000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x37b4d:$a: NanoCore • 0x37b5d:$a: NanoCore • 0x37d91:$a: NanoCore • 0x37da5:$a: NanoCore • 0x37de5:$a: NanoCore • 0x5fb6d:$a: NanoCore • 0x5fb7d:$a: NanoCore • 0x5fdb1:$a: NanoCore • 0x5fdc5:$a: NanoCore • 0x5fe05:$a: NanoCore • 0x37bac:$b: ClientPlugin • 0x37dae:$b: ClientPlugin • 0x37dee:$b: ClientPlugin • 0x5fbcc:$b: ClientPlugin • 0x5fdce:$b: ClientPlugin • 0x5fe0e:$b: ClientPlugin • 0x37cd3:$c: ProjectData • 0x5fcf3:$c: ProjectData • 0x386da:$d: DESCrypto • 0x606fa:$d: DESCrypto • 0x400a6:$e: KeepAlive

Click to see the 49 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
16.2.Peixoto - QUOTATION LIST.exe.71e0000.23.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x605:$x1: NanoCore.ClientPluginHost • 0x63e:$x2: IClientNetworkHost
16.2.Peixoto - QUOTATION LIST.exe.71e0000.23.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x605:$x2: NanoCore.ClientPluginHost • 0x720:$s4: PipeCreated • 0x61f:$s5: IClientLoggingHost
16.2.Peixoto - QUOTATION LIST.exe.71e0000.23.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2205:$x1: NanoCore.ClientPluginHost • 0x223e:$x2: IClientNetworkHost
16.2.Peixoto - QUOTATION LIST.exe.71e0000.23.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2205:$x2: NanoCore.ClientPluginHost • 0x2320:$s4: PipeCreated • 0x221f:$s5: IClientLoggingHost
16.2.Peixoto - QUOTATION LIST.exe.7180000.20.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
Click to see the 135 entries				

Sigma Overview

AV Detection:



Sigma detected: NanoCore

E-Banking Fraud:



Sigma detected: NanoCore

Stealing of Sensitive Information:



Sigma detected: NanoCore

Remote Access Functionality:



Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:



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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:



Yara detected Nanocore RAT

Copyright Joe Security LLC 2021

System Summary:



Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:



.NET source code contains potential unpacker

Boot Survival:



Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection:



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

HIPS / PFW / Operating System Protection Evasion:



Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:



Yara detected Nanocore RAT

Remote Access Functionality:



Detected Nanocore Rat

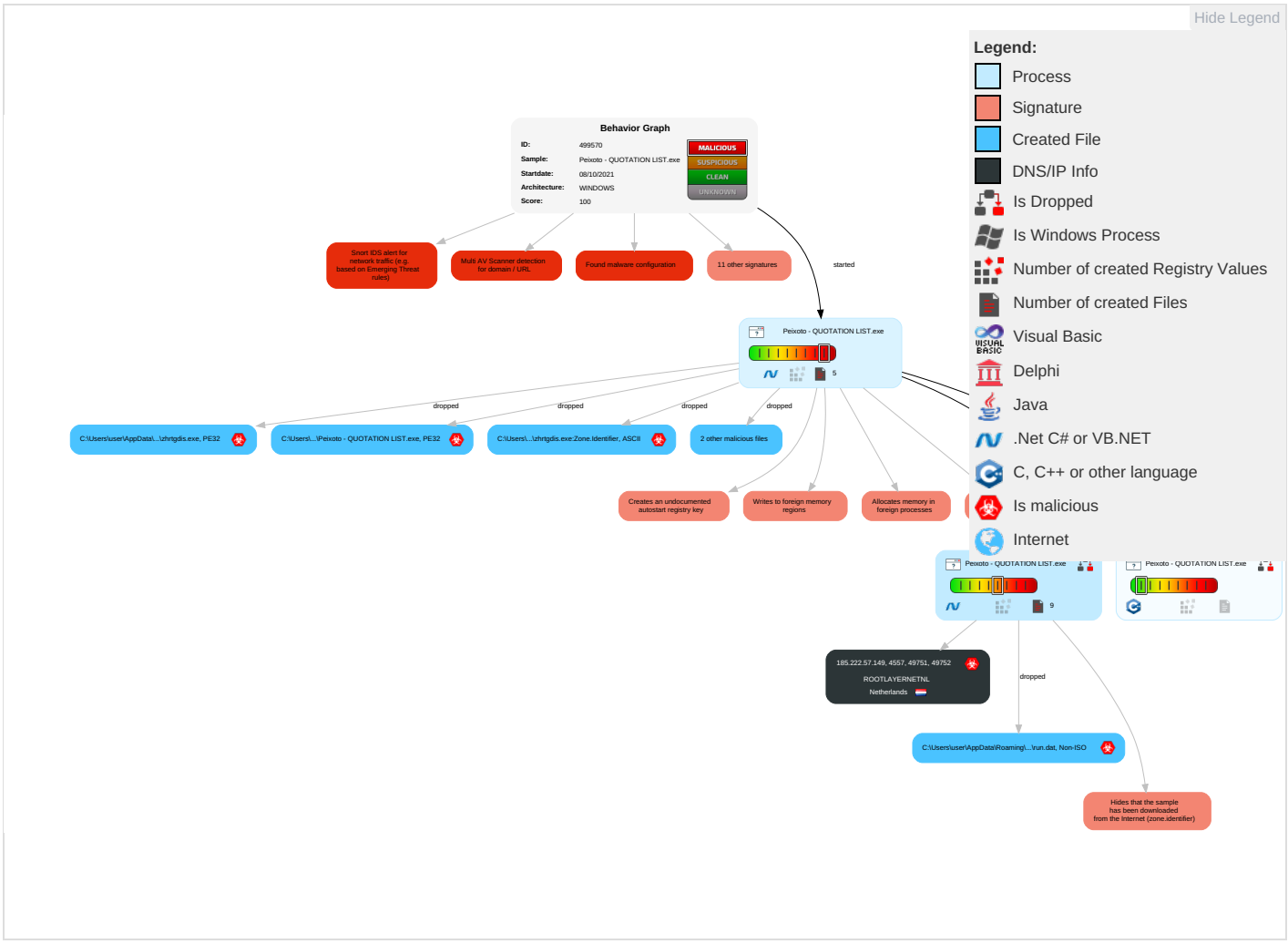
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Registry Run Keys / Startup Folder 1 1	Process Injection 3 1 2	Masquerading 1	Input Capture 2 1	Query Registry 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

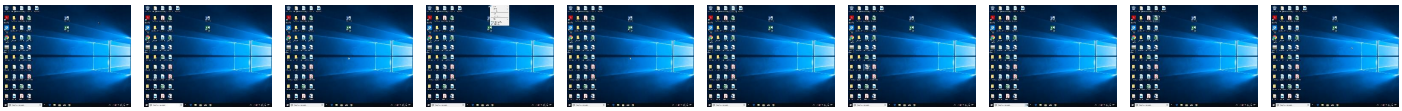
Behavior Graph



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
Peixoto - QUOTATION LIST.exe	26%	Virustotal		Browse
Peixoto - QUOTATION LIST.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Peixoto - QUOTATION LIST.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\zhrtgdis.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Peixoto - QUOTATION LIST.exe	26%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\zhrtgdis.exe	26%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.2.Peixoto - QUOTATION LIST.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.2.Peixoto - QUOTATION LIST.exe.6660000.17.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link	Download
16.2.Peixoto - QUOTATION LIST.exe.4448a20.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
127.0.0.1	0%	Virustotal		Browse
127.0.0.1	0%	Avira URL Cloud	safe	
185.222.57.149	6%	Virustotal		Browse
185.222.57.149	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
127.0.0.1	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
185.222.57.149	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.222.57.149	unknown	Netherlands		51447	ROOTLAYERNETNL	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	499570
Start date:	08.10.2021
Start time:	16:08:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Peixoto - QUOTATION LIST.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:	25
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

Copyright Joe Security LLC 2021

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@5/9@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 84.1% • Quality standard deviation: 10.6%
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

Simulations

Behavior and APIs

Time	Type	Description
16:09:56	API Interceptor	655x Sleep call for process: Peixoto - QUOTATION LIST.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.222.57.149	MERMAID SUBSEA - purchase order RX86404382953.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ROOTLAYERNETNL	SecuriteInfo.com.Trojan.Win32.Save.a.20322.exe	Get hash	malicious	Browse	• 45.137.22.115
	PaymentAdvice.exe	Get hash	malicious	Browse	• 185.222.58.151
	PI009876789.exe	Get hash	malicious	Browse	• 185.222.58.154
	Proforma invoice Shipping documents.exe	Get hash	malicious	Browse	• 45.137.22.91
	Payment_Advice.exe	Get hash	malicious	Browse	• 45.137.22.115
	PO. 2100002.xlsx	Get hash	malicious	Browse	• 185.222.57.162
	2WK7SGkGVZ.exe	Get hash	malicious	Browse	• 45.137.22.91
	PO1038845621.exe	Get hash	malicious	Browse	• 45.137.22.70
	SecuriteInfo.com.Suspicious.Win32.Save.a.24632.exe	Get hash	malicious	Browse	• 45.137.22.115
	Application Copy.exe	Get hash	malicious	Browse	• 45.137.22.70
	Swift Copy.xlsx	Get hash	malicious	Browse	• 185.222.57.85
	pre-shipment docs pdf.exe	Get hash	malicious	Browse	• 45.137.22.131
	SOA_SEPT.exe	Get hash	malicious	Browse	• 45.137.22.115
	MERMAID SUBSEA - purchase order RX86404382953.exe	Get hash	malicious	Browse	• 185.222.57.149
	Application copy.exe	Get hash	malicious	Browse	• 45.137.22.70
	New Purchase Order# 4502369263.exe	Get hash	malicious	Browse	• 45.137.22.142
	swift0098765.exe	Get hash	malicious	Browse	• 45.137.22.115
	bthGMpTA2L.exe	Get hash	malicious	Browse	• 185.222.58.118
	New Order PO200305-01.exe	Get hash	malicious	Browse	• 185.222.58.118

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO. 2100002.xlsx	Get hash	malicious	Browse	• 185.222.57.162

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Peixoto - QUOTATION LIST.exe.log

Process:	C:\Users\user\Desktop\Peixoto - QUOTATION LIST.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD D
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Temp\Peixoto - QUOTATION LIST.exe

Process:	C:\Users\user\Desktop\Peixoto - QUOTATION LIST.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1203200
Entropy (8bit):	7.928918657272288
Encrypted:	false
SSDEEP:	24576:Qi4th4HdHtaqrbvYfCxkRPaGynuJ4Bk0xdh1HVsx+aV3gyGw:P4tCvaqx0Ht+Bk0DNswq3g8
MD5:	0F129AA97048F7EC0557B211349A2CE0
SHA1:	B597185C94FAC60CD7E25DB83BFB39ED07409289
SHA-256:	FCF3B27FDC54C53A1F7510ABF8BDF748BD3199813D0294738FEBA29C7C1054D1
SHA-512:	0780847D48DDF9336633665560185E58C60BFD516D7CEB2139DE897C526E3D23236667A7BCC199009C37E1D8B153C40377D9717C51F97450967297F9D3BA759A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 26%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...[w.....0.....~..... .....@.. ....@.....O.....xz..... ....H.....text...4.... ....`.rsrc...xz.....|.....@..@.reloc..... .....Z.....@..B.....H.....$&.....>.....0..+..... .....+..(.....X...2.(.....&..*.....".....0..H.....(....o....+!..(.....r...p ..... .o....&..&....(....-.....o.....*.....+.....9.....0..U.....r...prS..prW..p(....(....rY..p .....%.(....(.....o....t.....s....%.o....o....*....0..Z.....(...rc..po!....s"....s#....o$.....o%.... .o&....o'.....io(.....,..o.....o)...s*...z.*.....-C.....

C:\Users\user\AppData\Local\Temp\Peixoto - QUOTATION LIST.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\Peixoto - QUOTATION LIST.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

C:\Users\user\AppData\Local\Temp\Peixoto - QUOTATION LIST.exe:Zone.Identifier	
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\AppData\Local\Temp\Peixoto - QUOTATION LIST.exe
File Type:	data
Category:	dropped
Size (bytes):	2088
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCe
MD5:	0D6805D12813A857D50D42D6EE2CCAB0
SHA1:	78D83F009D842F21FE2AB0EAFFD00E5AAD1776F4
SHA-256:	182E0F8AA959549D61C66D049645BA8445D86AEAD2B8C3552A9836FA1E5BD484
SHA-512:	5B29496F3AB3CCB915CF37042F4956BB00E577B5F15457A5A739BE1BD50C481FB7E3297EED575DCA7A7BD30ECBC140DD3666CD7DEDD25DFB7AEB41A1B5BEI A4A
Malicious:	false
Reputation:	moderate, very likely benign file
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\AppData\Local\Temp\Peixoto - QUOTATION LIST.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:5v8:G
MD5:	05D3210DC0F332DAC884A349CADDF7D9
SHA1:	7F6BCF10E578609F26A193EA92E72D57AE5EABC8
SHA-256:	384569455A5A7717A1CF73331CD40A9B2CE31AE8F4915351AA1FD8425E3B4C72
SHA-512:	DEEB972E54621868049FCA22E406B42F83C10305972DDEF7D9ED061F7DE90C3BBC12229A1477B0AEA0538847B2451C7211CE1A275508270F09CDED8525FDBA4
Malicious:	**true**
Reputation:	low
Preview:	).....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\AppData\Local\Temp\Peixoto - QUOTATION LIST.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
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\AppData\Local\Temp\Peixoto - QUOTATION LIST.exe

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
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
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\Microsoft\Windows\Start Menu\Programs\zhrtgdis.exe	
Process:	C:\Users\user\Desktop\Peixoto - QUOTATION LIST.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1203200
Entropy (8bit):	7.928918657272288
Encrypted:	false
SSDEEP:	24576:Qi4th4HdHtaqrbvYfCxkRPaGynuJ4Bk0xdh1HVsx+aV3gyGw:P4tCvaqx0Ht+Bk0DNswq3g8
MD5:	0F129AA97048F7EC0557B211349A2CE0
SHA1:	B597185C94FAC60CD7E25DB83BFB39ED07409289
SHA-256:	FCF3B27FDC54C53A1F7510ABF8BDF748BD3199813D0294738FEBA29C7C1054D1
SHA-512:	0780847D48DDF9336633665560185E58C60BFD516D7CEB2139DE897C526E3D23236667A7BCC199009C37E1D8B153C40377D9717C51F97450967297F9D3BA759A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 26%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...[w.....0.....~..... .....@.. ....@.....O.....xz..... ....H.....text...4.... ....`.rsrc...xz.....\|.....@..@.reloc..... .....Z.....@..B.....H.....$&.....>.....0..+..... .....+..(.....X...2.(.....&..*.....".....0..H.....(....o.....+!..(.....r...p ..... .o....&..&....(....-.....o....*.....+.....9.....0..U.....r...prS..prW..p(....(....rY..p .....%.(....(.....o....t.....s....%.o....o....*....0..Z.....(...rc..po!....s"....s#....o$.....o%.... .o&....o'.....io(.....,..o.....o)...s*...z.*.....-C.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\zhrtgdis.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Peixoto - QUOTATION LIST.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.928918657272288

General

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:	Peixoto - QUOTATION LIST.exe
File size:	1203200
MD5:	0f129aa97048f7ec0557b211349a2ce0
SHA1:	b597185c94fac60cd7e25db83bfb39ed07409289
SHA256:	fcf3b27fdc54c53a1f7510abf8bdf748bd3199813d0294738feba29c7c1054d1
SHA512:	0780847d48ddf9336633665560185e58c60bfd516d7ceb2139de897c526e3d23236667a7bcc199009c37e1d8b153c40377d9717c51f97450967297f9d3ba759a
SSDEEP:	24576:Qi4th4HdHtaqrbvYfCxkRPaGynuJ4Bk0xdh1HVsx+aV3gyGw:P4tCvaqx0Ht+Bk0DNswq3g8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...[w.....0.....~..... .....@.. .....@.....

File Icon



Icon Hash:	b296d2c2a2868682

Static PE Info

General

Entrypoint:	0x4efa2e
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:	0xAEA5775B [Mon Nov 6 22:59:39 2062 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xeda34	0xedc00	False	0.99087720163	data	7.99870340819	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xf0000	0x37a78	0x37c00	False	0.510588915359	data	7.04584846576	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x128000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/08/21-16:09:58.908995	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	4557	192.168.2.7	185.222.57.149
10/08/21-16:10:06.551810	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	4557	192.168.2.7	185.222.57.149
10/08/21-16:10:13.338507	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49773	4557	192.168.2.7	185.222.57.149
10/08/21-16:10:18.369904	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	4557	192.168.2.7	185.222.57.149
10/08/21-16:10:24.464828	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49780	4557	192.168.2.7	185.222.57.149
10/08/21-16:10:30.480115	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49781	4557	192.168.2.7	185.222.57.149
10/08/21-16:10:38.372617	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49782	4557	192.168.2.7	185.222.57.149
10/08/21-16:10:44.482585	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	4557	192.168.2.7	185.222.57.149
10/08/21-16:10:50.550682	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49801	4557	192.168.2.7	185.222.57.149
10/08/21-16:10:56.622820	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49813	4557	192.168.2.7	185.222.57.149
10/08/21-16:11:01.719619	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49814	4557	192.168.2.7	185.222.57.149
10/08/21-16:11:07.735436	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49815	4557	192.168.2.7	185.222.57.149
10/08/21-16:11:13.858199	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49816	4557	192.168.2.7	185.222.57.149

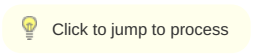
Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Peixoto - QUOTATION LIST.exe PID: 5460 Parent PID: 5540

Copyright Joe Security LLC 2021

General

Start time:	16:09:09
Start date:	08/10/2021
Path:	C:\Users\user\Desktop\Peixoto - QUOTATION LIST.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Peixoto - QUOTATION LIST.exe'
Imagebase:	0x20000
File size:	1203200 bytes
MD5 hash:	0F129AA97048F7EC0557B211349A2CE0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.331468267.000000000352B000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.331468267.000000000352B000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.331468267.000000000352B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.331768876.00000000035CA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.331768876.00000000035CA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.331768876.00000000035CA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.332453140.00000000036CA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.332453140.00000000036CA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.332453140.00000000036CA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.330874333.0000000002449000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.330874333.0000000002449000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Modified

Analysis Process: Peixoto - QUOTATION LIST.exe PID: 6572 Parent PID: 5460

General

Start time:	16:09:53
Start date:	08/10/2021
Path:	C:\Users\user\AppData\Local\Temp\Peixoto - QUOTATION LIST.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\Peixoto - QUOTATION LIST.exe
Imagebase:	0x10000

Copyright Joe Security LLC 2021

File size:	1203200 bytes
MD5 hash:	0F129AA97048F7EC0557B211349A2CE0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 26%, Virustotal, Browse
Reputation:	low

Analysis Process: Peixoto - QUOTATION LIST.exe PID: 6584 Parent PID: 5460

General

Start time:	16:09:53
Start date:	08/10/2021
Path:	C:\Users\user\AppData\Local\Temp\Peixoto - QUOTATION LIST.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Peixoto - QUOTATION LIST.exe
Imagebase:	0xeb0000
File size:	1203200 bytes
MD5 hash:	0F129AA97048F7EC0557B211349A2CE0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.507935886.0000000007200000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.507935886.0000000007200000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.508012010.0000000007240000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.508012010.0000000007240000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.507918779.00000000071F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.507918779.00000000071F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.508028677.0000000007250000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.508028677.0000000007250000.00000004.00020000.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.502803015.000000000345F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.507861382.00000000071D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.507861382.00000000071D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.505140332.0000000004437000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.506764545.0000000005CB0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.506764545.0000000005CB0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.507701529.0000000007170000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.507701529.0000000007170000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.497755666.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.497755666.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

	• Rule: NanoCore, Description: unknown, Source: 00000010.00000002.497755666.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.507798744.00000000071B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.507798744.00000000071B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.508130383.0000000007290000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.508130383.0000000007290000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.507974739.0000000007220000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.507974739.0000000007220000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.507735759.0000000007180000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.507735759.0000000007180000.00000004.00020000.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.505641453.00000000046D8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.507029930.0000000006660000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.507029930.0000000006660000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.507029930.0000000006660000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.502657660.00000000033E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.502657660.00000000033E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.507958323.0000000007210000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.507958323.0000000007210000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.507891553.00000000071E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.507891553.00000000071E0000.00000004.00020000.sdmp, Author: Florian Roth
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis