ID: 552140
Sample Name:
Z82M395C8INV0ICEPAYMENTC0PY.exe
Cookbook: default.jbs
Time: 22:34:56
Date: 12/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Z82M395C8INV0ICEPAYMENTC0PY.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
AV Detection: 5
E-Banking Fraud: 5
Stealing of Sensitive Information: 5
Remote Access Functionality: 5
Jbx Signature Overview 5
AV Detection: 6
Compliance: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 6
Data Obfuscation: 6
Hooking and other Techniques for Hiding and Protection: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
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
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 11
Dropped Files 11
Created / dropped Files 12
Static File Info 15
General 15
File Icon 16
Static PE Info 16
General 16
Entrypoint Preview 16
Rich Headers 16
Data Directories 16
Sections 16
Resources 16
Imports 16
Possible Origin 16
Network Behavior 17
Snort IDS Alerts 17
Network Port Distribution 17
TCP Packets 17
UDP Packets 17
DNS Queries 17
DNS Answers 18
Code Manipulations 19
Statistics 19

Behavior 19
System Behavior 19
Analysis Process: Z82M395C8INV0ICEPAYMENTC0PY.exe PID: 6756 Parent PID: 5344 19
General 19
File Activities 19
File Created 19
File Deleted 19
File Written 20
File Read 20
Registry Activities 20
Analysis Process: Z82M395C8INV0ICEPAYMENTC0PY.exe PID: 6912 Parent PID: 6756 20
General 20
File Activities 22
File Created 22
File Deleted 22
File Written 22
File Read 22
Analysis Process: anlq.exe PID: 7140 Parent PID: 3440 22
General 22
File Activities 22
File Created 22
File Deleted 22
File Written 22
File Read 22
Analysis Process: anlq.exe PID: 6252 Parent PID: 7140 22
General 22
File Activities 25
File Created 25
File Written 25
File Read 25
Analysis Process: anlq.exe PID: 6248 Parent PID: 3440 25
General 25
File Activities 25
File Created 25
File Deleted 25
File Written 25
File Read 25
Analysis Process: anlq.exe PID: 6216 Parent PID: 6248 25
General 25
File Activities 27
File Created 27
File Read 27
Disassembly 27
Code Analysis 27

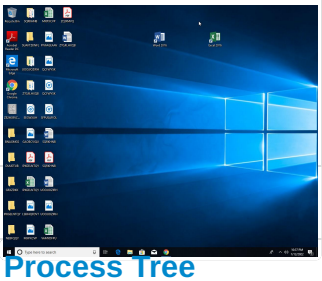
Windows Analysis Report Z82M395C8INV0ICEPAYMENT…

Overview

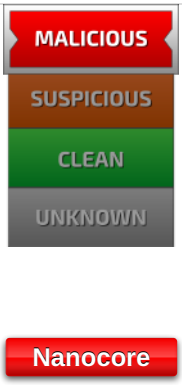
General Information

Sample Name:	Z82M395C8INV0ICEPAYMENTC0PY.exe
Analysis ID:	552140
MD5:	ed2d5d27e3d835..
SHA1:	cb0719235ebb92..
SHA256:	5214261c225f79d.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



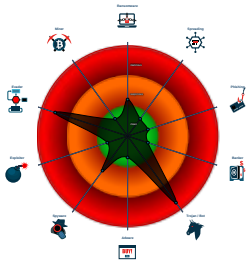
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Detected unpacking (creates a PE fi…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…

Classification



Process Tree

- **System is w10x64**
- Z82M395C8INV0ICEPAYMENTC0PY.exe (PID: 6756 cmdline: "C:\Users\user\Desktop\Z82M395C8INV0ICEPAYMENTC0PY.exe" MD5: ED2D5D27E3D835C59AF80720048BBA74)
  - Z82M395C8INV0ICEPAYMENTC0PY.exe (PID: 6912 cmdline: "C:\Users\user\Desktop\Z82M395C8INV0ICEPAYMENTC0PY.exe" MD5: ED2D5D27E3D835C59AF80720048BBA74)
- anlq.exe (PID: 7140 cmdline: "C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe" MD5: ED2D5D27E3D835C59AF80720048BBA74)
  - anlq.exe (PID: 6252 cmdline: "C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe" MD5: ED2D5D27E3D835C59AF80720048BBA74)
- anlq.exe (PID: 6248 cmdline: "C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe" MD5: ED2D5D27E3D835C59AF80720048BBA74)
  - anlq.exe (PID: 6216 cmdline: "C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe" MD5: ED2D5D27E3D835C59AF80720048BBA74)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.363442262.000000000414000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x111e5:$x1: NanoCore.ClientPluginHost • 0x11222:$x2: IClientNetworkHost • 0x14d55:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000002.00000000.363442262.000000000414000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000000.363442262.000000000414000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x10f4d:$a: NanoCore • 0x10f5d:$a: NanoCore • 0x11191:$a: NanoCore • 0x111a5:$a: NanoCore • 0x111e5:$a: NanoCore • 0x10fac:$b: ClientPlugin • 0x111ae:$b: ClientPlugin • 0x111ee:$b: ClientPlugin • 0x110d3:$c: ProjectData • 0x11ada:$d: DESCrypto • 0x194a6:$e: KeepAlive • 0x17494:$g: LogClientMessage • 0x1368f:$i: get_Connected • 0x11e10:$j: #=q • 0x11e40:$j: #=q • 0x11e5c:$j: #=q • 0x11e8c:$j: #=q • 0x11ea8:$j: #=q • 0x11ec4:$j: #=q • 0x11ef4:$j: #=q • 0x11f10:$j: #=q
00000002.00000002.625896770.000000000399 2000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000002.00000002.627827299.0000000004CB 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 109 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.anlq.exe.38f0e54.7.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
6.2.anlq.exe.38f0e54.7.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
6.2.anlq.exe.38f0e54.7.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
6.2.anlq.exe.415058.0.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
6.2.anlq.exe.415058.0.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
Click to see the 394 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:

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

Compliance:

- Detected unpacking (creates a PE file in dynamic memory)

Networking:

- Uses dynamic DNS services

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

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

Data Obfuscation:

- Detected unpacking (creates a PE file in dynamic memory)
- .NET source code contains potential unpacker

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:

- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Yara detected Nanocore RAT

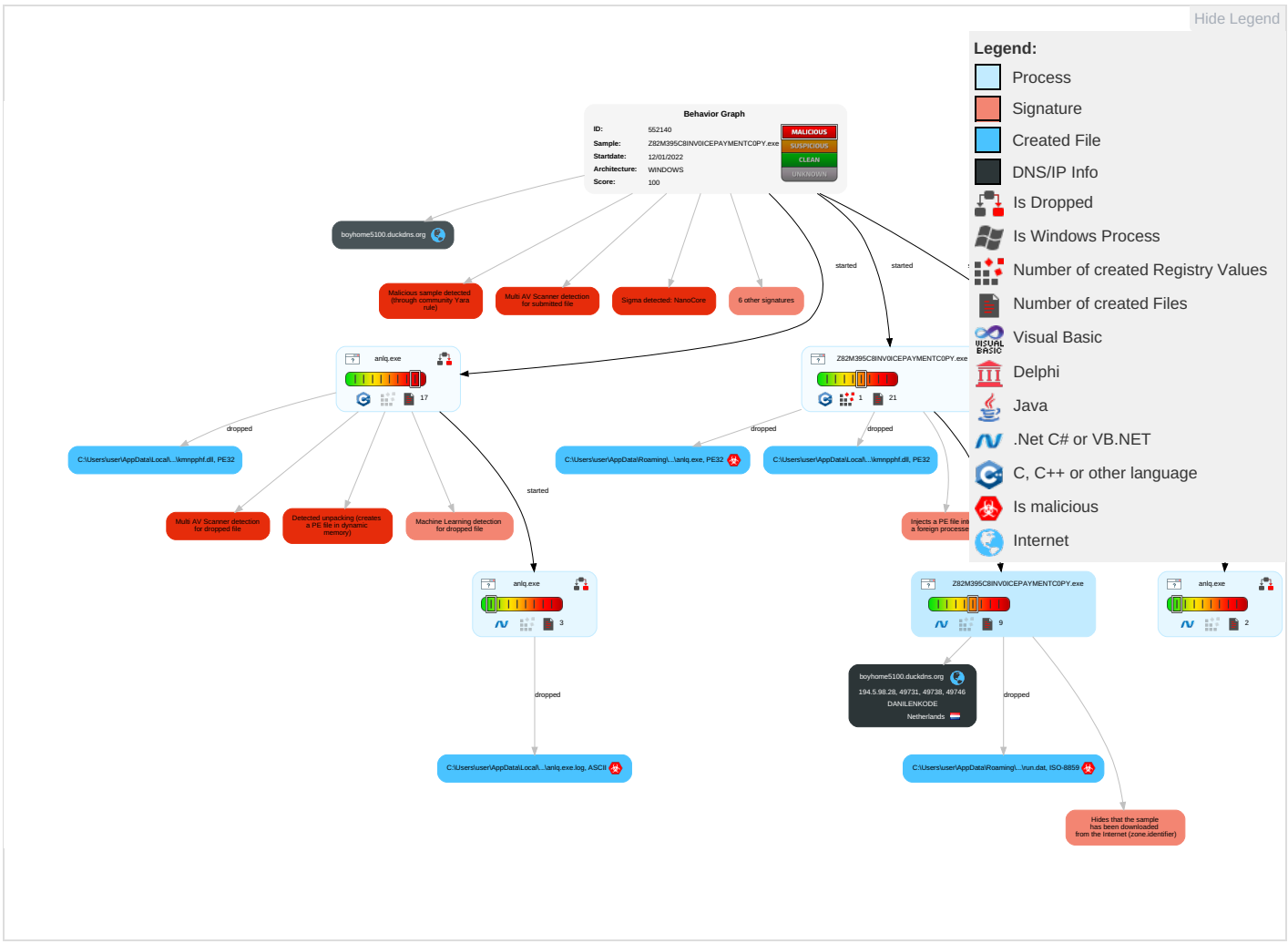
Remote Access Functionality:

- 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	Networl Effects
Valid Accounts	Native API 1	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdr Insecure Network Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 6	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Standard Port 1	Exploit S Track D Locatior
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 1	NTDS	Security Software Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 1 1	Jammin Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecure Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue C Base St

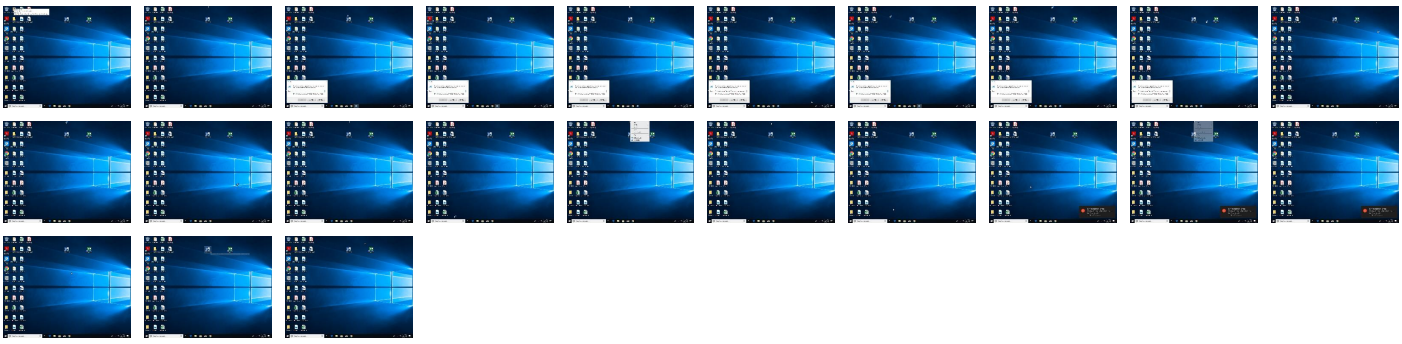
Behavior Graph



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
Z82M395C8INV0ICEPAYMENTC0PY.exe	35%	ReversingLabs	Win32.Backdoor.NanoBot	
Z82M395C8INV0ICEPAYMENTC0PY.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe	35%	ReversingLabs	Win32.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.anlq.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.anlq.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.0.anlq.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.anlq.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.0.anlq.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.Z82M395C8INV0ICEPAYMENTC0PY.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.anlq.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.2.anlq.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.0.anlq.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
6.0.anlq.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.0.Z82M395C8INV0ICEPAYMENTC0PY.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.Z82M395C8INV0ICEPAYMENTC0PY.exe.24d0000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.anlq.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.0.anlq.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.0.anlq.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.0.Z82M395C8INV0ICEPAYMENTC0PY.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.0.Z82M395C8INV0ICEPAYMENTC0PY.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.1.anlq.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.anlq.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.2.anlq.exe.4970000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.0.Z82M395C8INV0ICEPAYMENTC0PY.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.1.Z82M395C8INV0ICEPAYMENTC0PY.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.0.anlq.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.anlq.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.anlq.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.0.Z82M395C8INV0ICEPAYMENTC0PY.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.2.Z82M395C8INV0ICEPAYMENTC0PY.exe.31d0000.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.2.anlq.exe.4970000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.0.Z82M395C8INV0ICEPAYMENTC0PY.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.1.anlq.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.0.Z82M395C8INV0ICEPAYMENTC0PY.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
boyhome5100.duckdns.org	194.5.98.28	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.28	boyhome5100.duckdns.org	Netherlands		208476	DANILENKODE	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552140
Start date:	12.01.2022
Start time:	22:34:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 40s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	Z82M395C8INV0ICEPAYMENTC0PY.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/12@20/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 41.3% (good quality ratio 38.4%) • Quality average: 77.6% • Quality standard deviation: 30.5%
HCA Information:	• Successful, ratio: 90% • 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
22:35:58	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run pvlmhsolms C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe
22:36:04	API Interceptor	927x Sleep call for process: Z82M395C8INV0ICEPAYMENTC0PY.exe modified
22:36:06	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run pvlmhsolms C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe
22:36:14	API Interceptor	2x Sleep call for process: anlq.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\anlq.exe.log	
Process:	C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\mxscsgwl	
Process:	C:\Users\user\Desktop\Z82M395C8INV0ICEPAYMENTC0PY.exe
File Type:	data
Category:	dropped
Size (bytes):	7152
Entropy (8bit):	6.100652389310038
Encrypted:	false
SSDEEP:	192:pPJmOV/VtD9444/RZQS18oJ3v/dwF8AEaI0uL0BWZR:pBmuVT45yMr
MD5:	C72F32ACAA36B97D2C9CCA648E63550B
SHA1:	294DA546FECBAA319851256633C0B43EFA922342
SHA-256:	E867D5FE7A231EB1D1671282F37CA3416E3E00417A0E93D6FFDF1A7651F2D8FE
SHA-512:	21927F918F342047E4A44CCF0CB5FEFF1D9BD75645E849B1B2AA1BB452B22D78313D884A5F0C674FF8BFCB75F645104579A5FC4E10B37C4156A38B2924BEEAC
Malicious:	false
Reputation:	unknown
Preview:	!.....C*;*~...;.....&;.6...:.:.;.2.7..7..U.6.&....A..A..7..7..U.6.&&...A..A..7..7..U.6.&....A..A..7..7..U.6.&t...A..A..;.....QA..A."C..;&...A.&A.*C.&C.:U...../)C.&..:U..A.:..A .2;"...&....;.....:7...7...7..y.7..y.7...7.&.M,...C./..A.2.;$...7..y.C....A....:&.....;....C.2..C.....C-e...C*.....6C..C....C..C.C..C..A.6C...A.:C..C.~C..A.C.6C.:C-e....0<.&....&.....7..&.. .&.....S.&....&.....C*;*.....&..6...U..A.:;.6...C.:<..C.:~A.:C.6.A.6#"&...M...C..Q.....A...A...U.&Q.....A...A.....U.....7..&.....&..77A.2#.U.&.7..&.777A.2;.2...;...#.....C..C-e...C*;*~.....&..6..U..A.:;.6...C.:<..C.:~A.:C.6.A.6#"&...M..B@...C..Q.....A...A...C..Q.....A...A...C..Q....A...A...C.....A...A...U.&Q.....A...A.....U.....0<.&\....&.:77A.2;....C.&C ..A.#.7..7..7..7..7..&.477A.2;.2...;...#.....C..C-e...C*;*...6...U."A.:;.6...C.:<..C.:~A.:C.6.A.6#"&....M...C..Q.....A.."A..&C..Q.....A.."A..&.....U.."...S.&....&.:77A.2#.7.

C:\Users\user\AppData\Local\Temp\nse563.tmp	
Process:	C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe
File Type:	data
Category:	dropped
Size (bytes):	508823
Entropy (8bit):	7.283631809896216
Encrypted:	false
SSDEEP:	12288:Gqhfz1pHzv2+oe3cUknFYFD6TG9pjni6v:GqhHzv2uMjeACLv
MD5:	9F26D3663765833227F40CCD32F17D82
SHA1:	6965A27B59FD286E46C4BD4A537A297F7183BCC5
SHA-256:	8B5A1260BBE86C850088DC0FC409FF5F15CE0F0D88B813A7CB8FE0AC9387467C
SHA-512:	152B295FEA50D1A25DD19EBD12CFD1D09E323D36322B215C3488CB8F25E5972F18DEF78CA8B92DA759B292A96464903D3F6BD18E831FEF2B0E4190EFF7DE181 A
Malicious:	false
Reputation:	unknown
Preview:	.]....,.....G....E.....\.....]..... .....J.....j.....2.....(..... ....

C:\Users\user\AppData\Local\Temp\nse564.tmp\kmnpphf.dll	
Process:	C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	199168
Entropy (8bit):	5.81772341130579
Encrypted:	false
SSDEEP:	6144:BUtJEr7BQNzZ/vDXqxnfNahvFp1cck4X3rm6v:BnFYFD6TG9pjni6v
MD5:	62D3CFA1EB3CEB7A3907E88D85020AB0
SHA1:	56611CCF19214AFA5FCB93EB106897648C29EB5C
SHA-256:	AA8B47E733904E8BBB02236CA87CD54060D25540259DB1367BEB2A405F593A40
SHA-512:	721C9AE443B62FB6C555C5F60848A2E89B62CC806186D2A6D546ED53424C2CB3CAE97F5867A5F6DF76B29F8646B09A84680803D4179176955BC2D05FFFCDE2A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,...B...B...B.....B..C...B...C...B.a.F...B.a.B...B.d.....B.a.@...B.R ich..B.....PE..L.....a.....!.....@.....@..... .....0..x..... .....text...[..... ..`.rdata..2.....@..@.rsrc..... .....@..@.reloc..x....0.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsl2464.tmp	
Process:	C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe
File Type:	data
Category:	dropped
Size (bytes):	508823
Entropy (8bit):	7.283631809896216
Encrypted:	false
SSDEEP:	12288:Gqhfz1pHzv2+oe3cUknFYFD6TG9pjni6v:GqhHzv2uMjeACLv
MD5:	9F26D3663765833227F40CCD32F17D82
SHA1:	6965A27B59FD286E46C4BD4A537A297F7183BCC5
SHA-256:	8B5A1260BBE86C850088DC0FC409FF5F15CE0F0D88B813A7CB8FE0AC9387467C
SHA-512:	152B295FEA50D1A25DD19EBD12CFD1D09E323D36322B215C3488CB8F25E5972F18DEF78CA8B92DA759B292A96464903D3F6BD18E831FEF2B0E4190EFF7DE181 A
Malicious:	false
Reputation:	unknown
Preview:	.]....,.....G....E.....\.....].... .....J.....j.....2.....(..... ....

C:\Users\user\AppData\Local\Temp\nsl2465.tmp\kmnpphf.dll	
Process:	C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	199168
Entropy (8bit):	5.81772341130579
Encrypted:	false
SSDEEP:	6144:BUtJEr7BQNzZ/vDXqxnfNahvFp1cck4X3rm6v:BnFYFD6TG9pjni6v
MD5:	62D3CFA1EB3CEB7A3907E88D85020AB0
SHA1:	56611CCF19214AFA5FCB93EB106897648C29EB5C
SHA-256:	AA8B47E733904E8BBB02236CA87CD54060D25540259DB1367BEB2A405F593A40
SHA-512:	721C9AE443B62FB6C555C5F60848A2E89B62CC806186D2A6D546ED53424C2CB3CAE97F5867A5F6DF76B29F8646B09A84680803D4179176955BC2D05FFFCDE2A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,...B...B...B.....B..C...B...C...B.a.F...B.a.B...B.d.....B.a.@...B.R ich..B.....PE..L.....a.....!.....@.....@..... .....0..x..... .....text...[..... ..`.rdata..2.....@..@.rsrc..... .....@..@.reloc..x....0.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nslD79C.tmp	
Process:	C:\Users\user\Desktop\Z82M395C8INV0ICEPAYMENTC0PY.exe
File Type:	data
Category:	dropped
Size (bytes):	508823
Entropy (8bit):	7.283631809896216
Encrypted:	false

C:\Users\user\AppData\Local\Temp\nsID79C.tmp

SSDEEP:	12288:Gqhfz1pHzv2+oe3cUknFYFD6TG9pjni6v:GqhHzv2uMjeACLv
MD5:	9F26D3663765833227F40CCD32F17D82
SHA1:	6965A27B59FD286E46C4BD4A537A297F7183BCC5
SHA-256:	8B5A1260BBE86C850088DC0FC409FF5F15CE0F0D88B813A7CB8FE0AC9387467C
SHA-512:	152B295FEA50D1A25DD19EBD12CFD1D09E323D36322B215C3488CB8F25E5972F18DEF78CA8B92DA759B292A96464903D3F6BD18E831FEF2B0E4190EFF7DE181 A
Malicious:	false
Reputation:	unknown
Preview:	.]......,.....G....E.....\.....]..... ....J.....j.....2.....(..... ....

C:\Users\user\AppData\Local\Temp\nsvD7DB.tmp\kmnpphf.dll

Process:	C:\Users\user\Desktop\Z82M395C8INV0ICEPAYMENTC0PY.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	199168
Entropy (8bit):	5.81772341130579
Encrypted:	false
SSDEEP:	6144:BUtJEr7BQNzZ/vDXqxnfNahvFp1cck4X3rm6v:BnFYFD6TG9pjni6v
MD5:	62D3CFA1EB3CEB7A3907E88D85020AB0
SHA1:	56611CCF19214AFA5FCB93EB106897648C29EB5C
SHA-256:	AA8B47E733904E8BBB02236CA87CD54060D25540259DB1367BEB2A405F593A40
SHA-512:	721C9AE443B62FB6C555C5F60848A2E89B62CC806186D2A6D546ED53424C2CB3CAE97F5867A5F6DF76B29F8646B09A84680803D4179176955BC2D05FFFCDE2A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,...B...B...B.....B..C...B...C...B.a.F...B.a.B...B.d.....B.a.@...B.R ich..B.....PE..L.....a.....!.....@.....@..... .....0..x..... .....text...[..... ..`.rdata..2.....@..@.rsrc..... .....@..@.reloc..x....0.....@..B..... ....

C:\Users\user\AppData\Local\Temp\tyn45143l4wvfde

Process:	C:\Users\user\Desktop\Z82M395C8INV0ICEPAYMENTC0PY.exe
File Type:	data
Category:	dropped
Size (bytes):	278527
Entropy (8bit):	7.985502104470931
Encrypted:	false
SSDEEP:	3072:Z4+ZH5OraURNY8fEkDnK+bpMrqalBMh28AbwFflGP21otyTsd3xRayMVEFdRkroq:Z4CH52RTfEY1pHzhuw2rvqUbkCg3lOUF
MD5:	AB9DA07D0CE11856F399DAB21043B162
SHA1:	2494389F78F0E51ED23F6CBE2AF43550600520DE
SHA-256:	FA774C95C72700F55C8CEB3CC6BC15EB47D29386AB112D985963425DBA3B4B6F
SHA-512:	72672B3594AB35AF312D716A18E746D7CB6C8C486408D263D83ADBC479A20F2118BEA8B5A7879E547A4748E18D77AC3A79C912175CCE38F806153CC6374DBD2
Malicious:	false
Reputation:	unknown
Preview:	.X..G.@%.....V`..4.f...E|{..dR..`.;..u|.Q..E.1....k..3..\.....r..}e.....5.NRi.1..Q.`.*.....0..%1.v.t.../.....s...Jp...p.x9.....XzW.....\z ..a..gYL.pA>}.....V=C..D....."n.J...k...E..|.dfw.[. `.R.<..Tl...iO..R...ZH..?*.....r...[5)....@%x...J..C..p`....f....d...,d...`6...u|....E.B....k....2~n$.!.O\.r.....w.\..&..lc.....>.....9.0...e<}.....6.&....u.-.f..wBZ/....;.!e.)A..G.....;..?f..N..Ui*... .....x\?..%k...R..1.0....Q...>=..G3....<..<#m.fg.3..p...r...[.W....@%e...h...".V`h...f...E|{...R.7....M.|.h..E.;..u.k.p3.2.n$._.O..5...;...zw.\B....2k....Z..a..L....0.[.#.<..tV^H...6.&.i... ..E.wB..k,J;.!e..A..a.H.....FRN;.T.f.....*.....x.?..%k...R.E:.....Q...>=..G&t...<..<#m.fg.3..p...r...[5)....@%Q...$....V`....f...E|{..dR..`.;..u|.Q..E.1....k..3.2.n$._.O..5....K..w.\ ....c.....Z>.a..L....0.[...<}.....6.&.....wB..k,J;.!e.)A..G.....;..?f....Ui*.....x\?..%k...R.E:.....Q...>=..G&t..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat

Process:	C:\Users\user\Desktop\Z82M395C8INV0ICEPAYMENTC0PY.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKgmR7kkmefoeLBizbCuVkqYM:X4LDAnybgCFcps0OafmCYDlizZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005
SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF3851
Malicious:	false
Reputation:	unknown
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+ .2e'..E?.G.....[.&

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Z82M395C8INV0ICEPAYMENTC0PY.exe
File Type:	ISO-8859 text, with no line terminators, with overstriking
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:X8t:X8
MD5:	9D93C6CF90AB599A82A67A0AB371D993
SHA1:	AE25DF0939304BFA56F1B6F042F84FAD0E62295F
SHA-256:	E966467014C7CDEAB153A250AE636296672DCD71606E534BBCFCD40FFFC63764
SHA-512:	1B9BFA7B2B7EAC89D872806D0E23C42CA018CBB3A94743AD6A06E95C9F7966F2D8B3E9F55B14CAD2520024B54B38B3955D4597B10CE72AA739DA18526EEB6BC
Malicious:	**true**
Reputation:	unknown
Preview:	....^..H

C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe	
Process:	C:\Users\user\Desktop\Z82M395C8INV0ICEPAYMENTC0PY.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	630751
Entropy (8bit):	7.55799421480531
Encrypted:	false
SSDEEP:	12288:jpfbC8JP2OaDPme5DBeUB80He8KReH+vPXTvgAdyDoh7J:jJCp99BXBDHe8KRPrvgBDoD
MD5:	ED2D5D27E3D835C59AF80720048BBA74
SHA1:	CB0719235EBB92B6A5A7EAC6DD45BE182102860A
SHA-256:	5214261C225F79D92E2DE3D5FA6172DD95020DCA0592ED23840A396635FED7A6
SHA-512:	42CA58099881F9B141259DD84B09FA896427B0E1EBE0FC4362100C23010F45154F1C9F24A87F4EF6F39E6BF8A8C11921DA3758B6271EEE09121821927B870B10
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 35%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%..:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....Z.....%2.....p....@..... .....s.....R.....p.....tex t...vY.....Z..... ..`.rdata.....p.....^.....@..@.data.....p.....@....ndata.....@.....rsrc....R.....T...t.....@..@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.55799421480531
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Z82M395C8INV0ICEPAYMENTC0PY.exe
File size:	630751
MD5:	ed2d5d27e3d835c59af80720048bba74

General

SHA1:	cb0719235ebb92b6a5a7eac6dd45be182102860a
SHA256:	5214261c225f79d92e2de3d5fa6172dd95020dca0592ed23840a396635fed7a6
SHA512:	42ca58099881f9b141259dd84b09fa896427b0e1ebe0fc4362100c23010f45154f1c9f24a87f4ef6f39e6bf8a8c11921da3758b6271eee09121821927b870b10
SSDEEP:	12288:jpfbC8JP2OaDPme5DBeUB80He8KReH+vPXTvgAdyDoh7J:jJCp99BXBDHe8KRPrvgBDoD
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	d0d8c8c8ccdcd8c8

Static PE Info

General

Entrypoint:	0x403225
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x48EFCDC9 [Fri Oct 10 21:48:57 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5976	0x5a00	False	0.668619791667	data	6.46680044621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444878472222	data	5.17796812871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55078125	data	4.68983486809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x35280	0x35400	False	0.451254401408	data	6.13027794155	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/22-22:36:06.210831	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51774	8.8.8.8	192.168.2.6
01/12/22-22:36:12.664801	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56023	8.8.8.8	192.168.2.6
01/12/22-22:36:19.983352	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60261	8.8.8.8	192.168.2.6
01/12/22-22:36:26.270733	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56061	8.8.8.8	192.168.2.6
01/12/22-22:36:32.797931	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58336	8.8.8.8	192.168.2.6
01/12/22-22:36:39.070909	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52811	8.8.8.8	192.168.2.6
01/12/22-22:36:45.261274	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61374	8.8.8.8	192.168.2.6
01/12/22-22:36:58.187228	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50010	8.8.8.8	192.168.2.6
01/12/22-22:37:22.149820	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56628	8.8.8.8	192.168.2.6
01/12/22-22:37:32.685084	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59329	8.8.8.8	192.168.2.6
01/12/22-22:37:37.860119	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56129	8.8.8.8	192.168.2.6
01/12/22-22:37:44.459002	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58177	8.8.8.8	192.168.2.6
01/12/22-22:38:03.521722	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60211	8.8.8.8	192.168.2.6

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 12, 2022 22:36:06.097676992 CET	192.168.2.6	8.8.8.8	0xca1d	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:36:12.550487995 CET	192.168.2.6	8.8.8.8	0x4fba	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:36:19.871624947 CET	192.168.2.6	8.8.8.8	0xf46c	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:36:26.157471895 CET	192.168.2.6	8.8.8.8	0xe30a	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:36:32.684803009 CET	192.168.2.6	8.8.8.8	0x468f	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:36:38.956623077 CET	192.168.2.6	8.8.8.8	0xb235	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:36:45.147955894 CET	192.168.2.6	8.8.8.8	0x58f8	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:36:51.805424929 CET	192.168.2.6	8.8.8.8	0xa4d1	Standard query (0)	boyhome5100.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 12, 2022 22:36:58.074069977 CET	192.168.2.6	8.8.8.8	0xa7fd	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:02.842281103 CET	192.168.2.6	8.8.8.8	0x6993	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:09.328217030 CET	192.168.2.6	8.8.8.8	0xe999	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:15.649806976 CET	192.168.2.6	8.8.8.8	0xe276	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:22.036494970 CET	192.168.2.6	8.8.8.8	0x42bc	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:27.550156116 CET	192.168.2.6	8.8.8.8	0xca7a	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:32.572067022 CET	192.168.2.6	8.8.8.8	0x51c3	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:37.745713949 CET	192.168.2.6	8.8.8.8	0xd91f	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:44.343449116 CET	192.168.2.6	8.8.8.8	0xc655	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:50.772228003 CET	192.168.2.6	8.8.8.8	0xc1ec	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:57.092513084 CET	192.168.2.6	8.8.8.8	0xfb6c	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 22:38:03.410118103 CET	192.168.2.6	8.8.8.8	0x1481	Standard query (0)	boyhome510 0.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 12, 2022 22:36:06.210830927 CET	8.8.8.8	192.168.2.6	0xca1d	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:36:12.664800882 CET	8.8.8.8	192.168.2.6	0x4fba	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:36:19.983351946 CET	8.8.8.8	192.168.2.6	0xf46c	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:36:26.270733118 CET	8.8.8.8	192.168.2.6	0xe30a	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:36:32.797930956 CET	8.8.8.8	192.168.2.6	0x468f	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:36:39.070909023 CET	8.8.8.8	192.168.2.6	0xb235	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:36:45.261274099 CET	8.8.8.8	192.168.2.6	0x58f8	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:36:51.824903965 CET	8.8.8.8	192.168.2.6	0xa4d1	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:36:58.187227964 CET	8.8.8.8	192.168.2.6	0xa7fd	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:02.861450911 CET	8.8.8.8	192.168.2.6	0x6993	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:09.346029043 CET	8.8.8.8	192.168.2.6	0xe999	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:15.670027971 CET	8.8.8.8	192.168.2.6	0xe276	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:22.149820089 CET	8.8.8.8	192.168.2.6	0x42bc	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:27.568032980 CET	8.8.8.8	192.168.2.6	0xca7a	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:32.685084105 CET	8.8.8.8	192.168.2.6	0x51c3	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:37.860119104 CET	8.8.8.8	192.168.2.6	0xd91f	No error (0)	boyhome510 0.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 12, 2022 22:37:44.459002018 CET	8.8.8.8	192.168.2.6	0xc655	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:50.792978048 CET	8.8.8.8	192.168.2.6	0xc1ec	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:37:57.109962940 CET	8.8.8.8	192.168.2.6	0xfb6c	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 22:38:03.521722078 CET	8.8.8.8	192.168.2.6	0x1481	No error (0)	boyhome5100.duckdns.org		194.5.98.28	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Z82M395C8INV0ICEPAYMENTC0PY.exe PID: 6756 Parent PID: 5344

General

Start time:	22:35:55
Start date:	12/01/2022
Path:	C:\Users\user\Desktop\Z82M395C8INV0ICEPAYMENTC0PY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Z82M395C8INV0ICEPAYMENTC0PY.exe"
Imagebase:	0x400000
File size:	630751 bytes
MD5 hash:	ED2D5D27E3D835C59AF80720048BBA74
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.365884798.0000000003180000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.365884798.0000000003180000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.365884798.0000000003180000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.365884798.0000000003180000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Analysis Process: Z82M395C8INV0ICEPAYMENTC0PY.exe PID: 6912 Parent PID: 6756

General

Start time:	22:35:57
Start date:	12/01/2022
Path:	C:\Users\user\Desktop\Z82M395C8INV0ICEPAYMENTC0PY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Z82M395C8INV0ICEPAYMENTC0PY.exe"
Imagebase:	0x400000
File size:	630751 bytes
MD5 hash:	ED2D5D27E3D835C59AF80720048BBA74
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: 00000002.00000000.363442262.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000000.363442262.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000000.363442262.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.625896770.0000000003992000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.627827299.0000000004CB0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.627827299.0000000004CB0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.627227835.0000000004A70000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.627227835.0000000004A70000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.623964135.0000000002901000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000001.364412738.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000001.364412738.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000001.364412738.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.622759427.0000000000A20000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.622759427.0000000000A20000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.622759427.0000000000A20000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.622759427.0000000000A20000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.620999769.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.620999769.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.620999769.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.620999769.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000000.361866032.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000000.361866032.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000000.361866032.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.623549794.00000000024D2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.623549794.00000000024D2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.623549794.00000000024D2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.621386474.00000000004F5000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.621386474.00000000004F5000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.621386474.00000000004F5000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: anlq.exe PID: 7140 Parent PID: 3440

General

Start time:	22:36:06
Start date:	12/01/2022
Path:	C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe"
Imagebase:	0x400000
File size:	630751 bytes
MD5 hash:	ED2D5D27E3D835C59AF80720048BBA74
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.404828748.0000000002540000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.404828748.0000000002540000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.404828748.0000000002540000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.404828748.0000000002540000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 35%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: anlq.exe PID: 6252 Parent PID: 7140

General

Start time:	22:36:14
Start date:	12/01/2022
Path:	C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe"
Imagebase:	0x400000

File size:	630751 bytes
MD5 hash:	ED2D5D27E3D835C59AF80720048BBA74
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: 00000004.00000002.426987526.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.426987526.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.426987526.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.426987526.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.427356055.0000000000566000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.427356055.0000000000566000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.427356055.0000000000566000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.428146647.00000000037D1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.428146647.00000000037D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.428146647.00000000037D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000001.403510714.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000001.403510714.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000001.403510714.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.400147731.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.400147731.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.400147731.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.402469401.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.402469401.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.402469401.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.428239415.000000000380A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.428239415.000000000380A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.428060388.00000000027DE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.428633654.0000000004972000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.428633654.0000000004972000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.428633654.0000000004972000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.428567039.0000000004920000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.428567039.0000000004920000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.428567039.0000000004920000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.428567039.0000000004920000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: anlq.exe PID: 6248 Parent PID: 3440

General

Start time:	22:36:14
Start date:	12/01/2022
Path:	C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe"
Imagebase:	0x400000
File size:	630751 bytes
MD5 hash:	ED2D5D27E3D835C59AF80720048BBA74
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.413977938.0000000002240000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.413977938.0000000002240000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.413977938.0000000002240000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.413977938.0000000002240000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: anlq.exe PID: 6216 Parent PID: 6248

General

Start time:	22:36:17
Start date:	12/01/2022
Path:	C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe"
Imagebase:	0x400000
File size:	630751 bytes
MD5 hash:	ED2D5D27E3D835C59AF80720048BBA74
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: 00000006.00000002.429444309.0000000000545000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.429444309.0000000000545000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.429444309.0000000000545000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.429279463.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.429279463.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.429279463.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.429279463.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.430125055.000000000287E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000000.411198452.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000000.411198452.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000000.411198452.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.430201421.00000000038AA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.430201421.00000000038AA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.430159374.0000000003871000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.430159374.0000000003871000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.430159374.0000000003871000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000001.412926544.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000001.412926544.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000001.412926544.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.430288597.0000000004972000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.430288597.0000000004972000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.430288597.0000000004972000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.430024527.00000000024C0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.430024527.00000000024C0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.430024527.00000000024C0000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.430024527.00000000024C0000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000000.410019123.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000000.410019123.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000000.410019123.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis