ID: 551967
Sample Name:
039846H0INVOICERECEIPT.exe
Cookbook: default.jbs
Time: 18:37:12
Date: 12/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

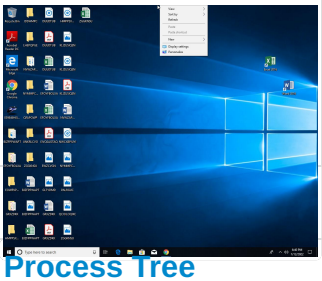
Windows Analysis Report 039846H0INVOICERECEIPT.exe

Overview

General Information

Sample Name:	039846H0INVOICERECEIPT.exe
Analysis ID:	551967
MD5:	3ba78ed2e621b7..
SHA1:	d735536d9984db..
SHA256:	329def14e6fa2aa..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

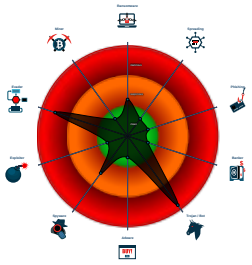
Nanocore

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

Signatures

- Found malware configuration
- 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 …
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w10x64**
- 039846H0INVOICERECEIPT.exe (PID: 5220 cmdline: "C:\Users\user\Desktop\039846H0INVOICERECEIPT.exe" MD5: 3BA78ED2E621B7BB47778EC2567DF223)
  - 039846H0INVOICERECEIPT.exe (PID: 4396 cmdline: "C:\Users\user\Desktop\039846H0INVOICERECEIPT.exe" MD5: 3BA78ED2E621B7BB47778EC2567DF223)
- anlq.exe (PID: 3224 cmdline: "C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe" MD5: 3BA78ED2E621B7BB47778EC2567DF223)
  - anlq.exe (PID: 6196 cmdline: "C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe" MD5: 3BA78ED2E621B7BB47778EC2567DF223)
- anlq.exe (PID: 6332 cmdline: "C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe" MD5: 3BA78ED2E621B7BB47778EC2567DF223)
  - anlq.exe (PID: 6392 cmdline: "C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe" MD5: 3BA78ED2E621B7BB47778EC2567DF223)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "c6aea8ec-42ab-4933-970f-cf8fecc5",
  "Group": "",
  "Domain1": "girlhomejan6100.duckdns.org",
  "Domain2": "girlhomejan6100.duckdns.org",
  "Port": 6100,
  "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
0000000B.00000000.294082200.000000000414000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x111e5:$x1: NanoCore.ClientPluginHost • 0x11222:$x2: IClientNetworkHost • 0x14d55:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000B.00000000.294082200.000000000414000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000B.00000000.294082200.000000000414000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x10f4d:$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
00000001.00000002.508293325.000000000390000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.508293325.000000000390 4000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x7601:$a: NanoCore • 0x765a:$a: NanoCore • 0x7697:$a: NanoCore • 0x7710:$a: NanoCore • 0x1adbb:$a: NanoCore • 0x1add0:$a: NanoCore • 0x1ae05:$a: NanoCore • 0x24c69:$a: NanoCore • 0x24cc2:$a: NanoCore • 0x24cff:$a: NanoCore • 0x24d78:$a: NanoCore • 0x38423:$a: NanoCore • 0x38438:$a: NanoCore • 0x3846d:$a: NanoCore • 0x46082:$a: NanoCore • 0x460a7:$a: NanoCore • 0x46100:$a: NanoCore • 0x7663:$b: ClientPlugin • 0x76a0:$b: ClientPlugin • 0x7f9e:$b: ClientPlugin • 0x7fab:$b: ClientPlugin
Click to see the 104 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.039846H0INVOICERECEIPT.exe.38e1aec.12.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10937:$x1: NanoCore.ClientPluginHost • 0x10951:$x2: IClientNetworkHost
1.2.039846H0INVOICERECEIPT.exe.38e1aec.12.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x10937:$x2: NanoCore.ClientPluginHost • 0x13c74:$s4: PipeCreated • 0x10924:$s5: IClientLoggingHost
0.2.039846H0INVOICERECEIPT.exe.31b1458.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.039846H0INVOICERECEIPT.exe.31b1458.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
0.2.039846H0INVOICERECEIPT.exe.31b1458.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 412 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 dropped file
- Yara detected Nanocore RAT

Compliance:

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

Networking:

- C2 URLs / IPs found in malware configuration
- 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:

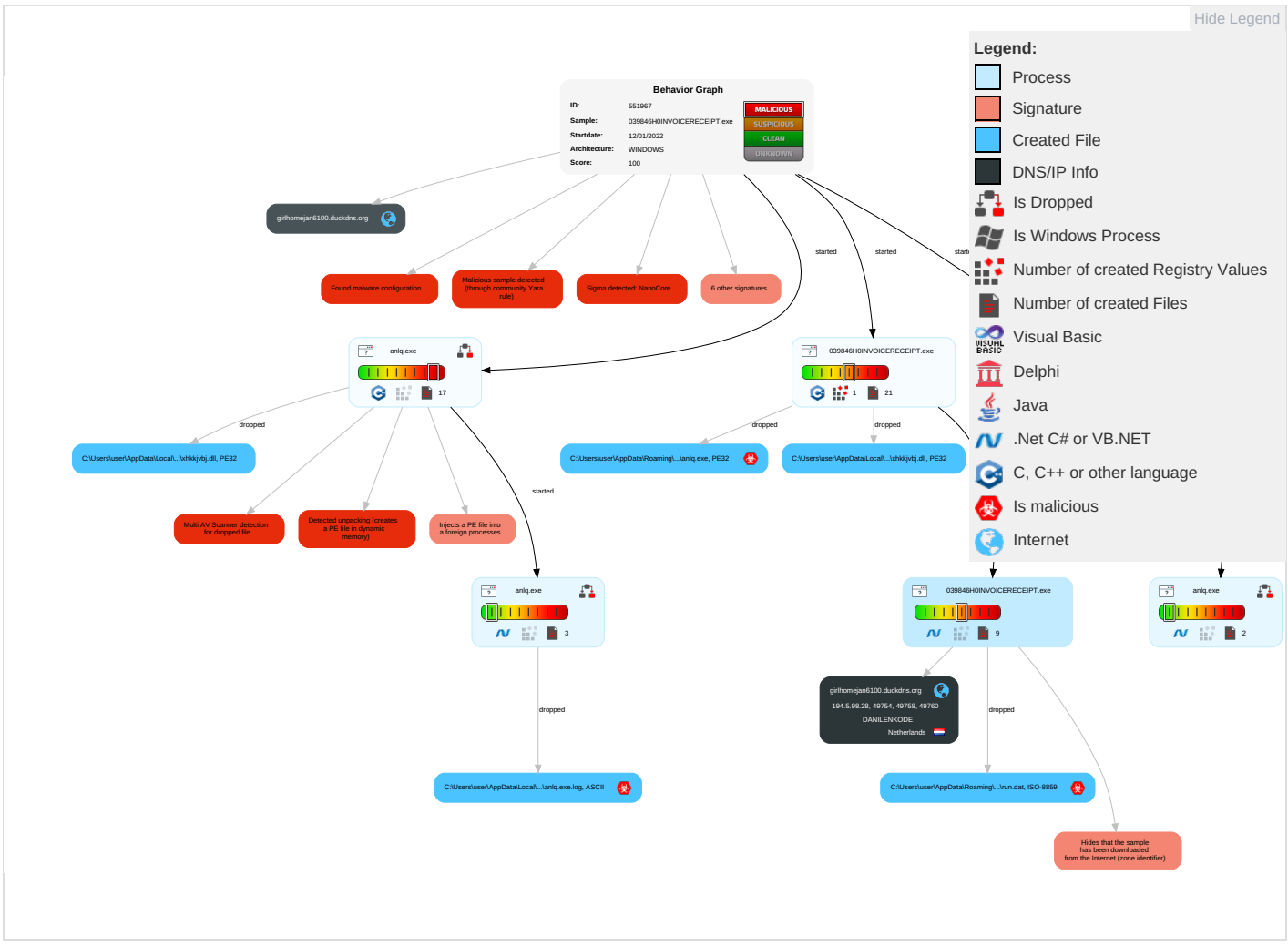
- Detected Nanocore Rat
- Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Native API 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Disable or Modify Tools 1	Input Capture 2 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdı Insecur Networ Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 5	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Remote Access Software 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 1	NTDS	Security Software Discovery 1 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 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	Multiband Communication	Jammin Denial c Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	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	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protoco

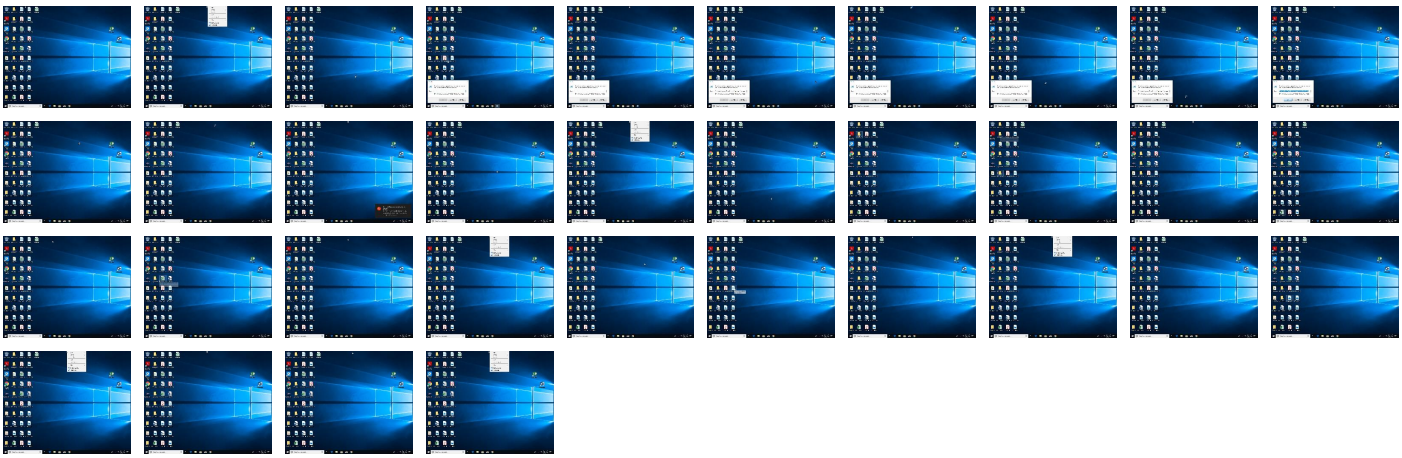
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe	33%	ReversingLabs	Win32.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.0.anlq.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.anlq.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.0.039846H0INVOICERECEIPT.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.039846H0INVOICERECEIPT.exe.31f0000.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.0.anlq.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.anlq.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.anlq.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.anlq.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.anlq.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.anlq.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.anlq.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.2.039846H0INVOICERECEIPT.exe.24e0000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
1.0.039846H0INVOICERECEIPT.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.0.039846H0INVOICERECEIPT.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.anlq.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.anlq.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.anlq.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.anlq.exe.22e0000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.anlq.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.1.anlq.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.anlq.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.0.039846H0INVOICERECEIPT.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.0.039846H0INVOICERECEIPT.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.2.039846H0INVOICERECEIPT.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.anlq.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.0.039846H0INVOICERECEIPT.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.anlq.exe.2650000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.anlq.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.0.039846H0INVOICERECEIPT.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
girlhomejan6100.duckdns.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
girlhomejan6100.duckdns.org	194.5.98.28	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
girlhomejan6100.duckdns.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.28	girlhomejan6100.duckdns.org	Netherlands		208476	DANILENKODE	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	551967
Start date:	12.01.2022
Start time:	18:37:12
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 13m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	039846H0INVOICERECEIPT.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:	31
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@19/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 49.3% (good quality ratio 44.7%) • Quality average: 75.3% • Quality standard deviation: 32.6%
HCA Information:	• Successful, ratio: 89% • 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
18:38:07	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run pvlmhsolms C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe
18:38:13	API Interceptor	919x Sleep call for process: 039846H0INVOICERECEIPT.exe modified
18:38:17	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run pvlmhsolms C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe
18:38:19	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\hrggihx	
Process:	C:\Users\user\Desktop\039846H0INVOICERECEIPT.exe
File Type:	data
Category:	dropped
Size (bytes):	7272
Entropy (8bit):	6.09209206442148
Encrypted:	false
SSDEEP:	192:8kkYa0Nt5QUVWRwieW9MUAaEv5dkuugi16h:KYIRwIdAb5dkuuVA
MD5:	84AF91836496FCF1039B4EF1849BCCCC
SHA1:	6AAFD320AE47429F68E325060D816F8055510269
SHA-256:	3048FF8B8E6228D2AFFC852697C81DF5FC8CF44FBC63AC3592F199334F592FAE
SHA-512:	7BEA193F17D21BA3A63A3010DFE8C09E4B45E9C846ED8FD1106342BCE7FCC89DEEBE9F8BD03FDF41F5D9D7EFF4516D61D1F9515B5B289E0F18B62D3B9687B96
Malicious:	false
Reputation:	unknown
Preview:	..~}},...="+....}.....b<.....b<....}.<.e}}}...}.....m.<.-..}}}.<..,.....m.<.-..}}}.<..,.....m.<.-..}}}.<..,.....m.<.-..}}}.<..,...my.W'.5..rr<...<..,..<m.yB..<..D..<..D..y.B.'m8...<.r,..y..<..+...'B.}}}}.yY|.Z.....8...7...@5...@8...6...3...m.E....E.A.].....@7.<..|.<.r...}}}}.9YyR}}}.yY.....36.<.63*..4..},..00.....b<..<..}J<..].<..}.Dm.i.,..9.y.<..<..}=.D....<..,...4..}%k.....}}.#.}}.i}%.....}}.1.}}..}%.1...).}}.G.}}..},...e.....b<..<.m}}}.<..<....}.k.<..}}.<.=.<..<.E.<....i}}}...;.<..'.8..}.9...)...<..'.8..}.9...)..'.'.5..}.9|.-%.....}}-.....<....<.-....G....<....}.{...}.~.<..}}}.<...4.y},...=.....b<..<.e}}}.<..<....}.k.<..}}.<.=.<..<.E.<.....y}}.....}}}.<..'.8..}.9...)...<..'.8..}.9...)...<m.'.8...9...)...<iB.'.7..r.9I..AI..<..'.8....9...)..'|'.5..}.9|.-%k.....}}}-.....<...u}...<..Du...n..u..i..m.....N....<....}.{...}.~.<..}}}.<...4.i},...q.<.m}}}.<..<....}.k.<..}}.<.=.<..<.E.<....'r}}...;.<..'.8..}.9...)...<..'.8..}.9...)..'.'.5..}.9|.-%.1...^}}}-.Y....<.....

C:\Users\user\AppData\Local\Temp\lbzyziajixj	
Process:	C:\Users\user\Desktop\039846H0INVOICERECEIPT.exe
File Type:	data
Category:	dropped
Size (bytes):	278527
Entropy (8bit):	7.98626113376592
Encrypted:	false
SSDEEP:	6144:EVfOvppvVrqXcEI6r/dlwsH0L+lBzusPxqeaz0Q/uZy07iF0O:EUvpeXcbRLsBzuSQj0Q21GF0O
MD5:	1A877E28204D5F93FA7C6741EF0388A5
SHA1:	FD6AFFA1F9A8C1A0D5FDDE565A45B83083A20F51
SHA-256:	53021B4269BB956F3FC824666A1C064B359038E4148C4C3FED3BF00C5BC8AFA4
SHA-512:	1E38B92109EFE988EB1109806C3DC78C35FDFA05601874F6621B1AA789CE67C131981D2C2E4F0C0301BA1C901638AB90EE5B23F9917161480FAF79111C432EA3
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\lbzyziajixj	
Preview:	....(<[a-..^..I.2.:%x..+..]........C.\.J.L...qr..w.9.'..% ..k.*.fA...$og.u.%.?.Y[.....Y...`..I...gC!.DXBB?..J..%.p..F...}j.........z[]6...'.$...........e.0hdeI.6.?.|.....E....!..zg.K;1.@Y..T..L....Dp.. I.>.o.....Z.Ts.|..0.vq..y.....D...&.Jv..6K.a<[a8?.^...]...x..N....(.$.CQ\.J.....qn|.w...'..% .2.y.^... v|...`-\..X...v'.F...........V.*m.e,h..;....N....j...........~..........b..YD.3..#.9..,...#.#dj..h.....#.". ...R..0.......%3w..|(.x..+V...Rt1....6...H.v6..M.D.H.......7...&.Jv.Z#.|.<[a.N.^..I...:%x..N..]........&.\.n.Z.:".q.>.w...'..% ..k.yP^... v....`-5....v'.22.........O8..V..m.d,h....9..n./.........qv.... ~'W.........b..YD.3....\l.,....#dc-....#.."....R..0..a..'..%3w..|J....+V...Rt1....../..v6..M.D.H.......7...&.Jv..6K.a<[a...^.kI...:%x..N..]........C.\.J.L...qr..w.9.'..% .2k.yP^... v....`-\j....v'.2.. .......O...V..m.d,h.........N...}j..........~'.........b..YD.3..#.9..,...#.#dj../....#."....R..0.........%3w..|J....+V...Rt1....../..v

C:\Users\user\AppData\Local\Temp\nsa26F.tmp	
Process:	C:\Users\user\Desktop\039846H0INVOICERECEIPT.exe
File Type:	data
Category:	dropped
Size (bytes):	512250
Entropy (8bit):	7.256628469673656
Encrypted:	false
SSDEEP:	12288:oUvpeXcbRLsBzuSQj0Q21GF06nCYFD6TG9pjni6v:BRalzC03AFNTACLv
MD5:	034F48DF0C0D4EE3A38B94F6DA5C1AC0
SHA1:	A58C49CC5CBD163FF1761694925F0456710BBDBA
SHA-256:	4D8989CEF3C0C56870D6155502AE3502A7AA8A0CB1710CEEF3CE90DED224CA24
SHA-512:	6E96F7D84FA31F4AD7262E781262AD4309B3EFB16609A5932449D0F300B7277780A66FD4F7D291E99AEFA557DAF3F2DB2B24E535DB53C854B8E7D789C77C817F
Malicious:	false
Reputation:	unknown
Preview:	.j.....,.....|...IO.....i.....kj.....'..... .....J.....!...j.....?..... ....

C:\Users\user\AppData\Local\Temp\nsa270.tmp\xhkkjvbj.dll	
Process:	C:\Users\user\Desktop\039846H0INVOICERECEIPT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	199168
Entropy (8bit):	5.816916948044661
Encrypted:	false
SSDEEP:	6144:SUtJEr7mQNzZ/vDXqxnfNahvFp1cck4X3rm6v:SnCYFD6TG9pjni6v
MD5:	4ABDC13A9B62E3DA21D83E864F3B865F
SHA1:	7892B7FA56E730DE7E08F23E5808DFB915C1FF23
SHA-256:	E3A428A341B65CC607F5C48109502B3D1DACEA9275F0471FE451EC06DFD8B0A4
SHA-512:	413B53E7427F5132C92FC3ECB0AF329334C285E3D0244D61A50764FB53A642151FD2FA214EDAFC1CC3703D22D97CC8A4DEB997005E3EBE52541D9DE74E39E9 D
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...K..... ..`.rdata.....@..@.rsrc..... .....@..@.reloc..x....0.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsa59C7.tmp	
Process:	C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe
File Type:	data
Category:	dropped
Size (bytes):	512250
Entropy (8bit):	7.256628469673656
Encrypted:	false
SSDEEP:	12288:oUvpeXcbRLsBzuSQj0Q21GF06nCYFD6TG9pjni6v:BRalzC03AFNTACLv
MD5:	034F48DF0C0D4EE3A38B94F6DA5C1AC0
SHA1:	A58C49CC5CBD163FF1761694925F0456710BBDBA
SHA-256:	4D8989CEF3C0C56870D6155502AE3502A7AA8A0CB1710CEEF3CE90DED224CA24
SHA-512:	6E96F7D84FA31F4AD7262E781262AD4309B3EFB16609A5932449D0F300B7277780A66FD4F7D291E99AEFA557DAF3F2DB2B24E535DB53C854B8E7D789C77C817F
Malicious:	false
Reputation:	unknown
Preview:	.j.....,.....|...IO.....i.....kj.....'..... .....J.....!...j.....?..... ....

C:\Users\user\AppData\Local\Temp\nsn3AA6.tmp	
Process:	C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe
File Type:	data
Category:	dropped
Size (bytes):	512250
Entropy (8bit):	7.256628469673656
Encrypted:	false
SSDEEP:	12288:oUvpeXcbRLsBzuSQj0Q21GF06nCYFD6TG9pjni6v:BRalzC03AFNTACLv
MD5:	034F48DF0C0D4EE3A38B94F6DA5C1AC0
SHA1:	A58C49CC5CBD163FF1761694925F0456710BBDBA
SHA-256:	4D8989CEF3C0C56870D6155502AE3502A7AA8A0CB1710CEEF3CE90DED224CA24
SHA-512:	6E96F7D84FA31F4AD7262E781262AD4309B3EFB16609A5932449D0F300B7277780A66FD4F7D291E99AEFA557DAF3F2DB2B24E535DB53C854B8E7D789C77C817F
Malicious:	false
Reputation:	unknown
Preview:	.j.....,.....|...lO.....i.....kj.....'..... .....J.....!..j.....?..... ....

C:\Users\user\AppData\Local\Temp\nsn3AA7.tmp\xhkkjvbj.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):	5.816916948044661
Encrypted:	false
SSDEEP:	6144:SUtJEr7mQNzZ/vDXqxnfNahvFp1cck4X3rm6v:SnCYFD6TG9pjni6v
MD5:	4ABDC13A9B62E3DA21D83E864F3B865F
SHA1:	7892B7FA56E730DE7E08F23E5808DFB915C1FF23
SHA-256:	E3A428A341B65CC607F5C48109502B3D1DACEA9275F0471FE451EC06DFD8B0A4
SHA-512:	413B53E7427F5132C92FC3ECB0AF329334C285E3D0244D61A50764FB53A642151FD2FA214EDAFC1CC3703D22D97CC8A4DEB997005E3EBE52541D9DE74E39E9 D
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...K..... ..`.rdata.....@..@.rsrc..... .....@..@.reloc..x....0.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsv59F7.tmp\xhkkjvbj.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):	5.816916948044661
Encrypted:	false
SSDEEP:	6144:SUtJEr7mQNzZ/vDXqxnfNahvFp1cck4X3rm6v:SnCYFD6TG9pjni6v
MD5:	4ABDC13A9B62E3DA21D83E864F3B865F
SHA1:	7892B7FA56E730DE7E08F23E5808DFB915C1FF23
SHA-256:	E3A428A341B65CC607F5C48109502B3D1DACEA9275F0471FE451EC06DFD8B0A4
SHA-512:	413B53E7427F5132C92FC3ECB0AF329334C285E3D0244D61A50764FB53A642151FD2FA214EDAFC1CC3703D22D97CC8A4DEB997005E3EBE52541D9DE74E39E9 D
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...K..... ..`.rdata.....@..@.rsrc..... .....@..@.reloc..x....0.....@..B..... ....

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\039846H0INVOICERECEIPT.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.089541637477408

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKgmR7kkmefoeLBizbCuVkqYM:X4LDAnybgCFcps0OafmCYDlizZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005
SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF385 1
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\039846H0INVOICERECEIPT.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Vrbe8:BbR
MD5:	0E68D78A36EF2C6EF8D21982A69E2B8E
SHA1:	D068EAEA77750FBF39FCD3745518AEF1299C923A
SHA-256:	1627BB8E1FA328D1BFAA1E4886DAB9402AC843228F4884FDA87EFDFEB43A19E7
SHA-512:	E617DE5DDB17E673F1B77C9730E33A2360BAD48D66796ED1A539E9F52C14B62F96F8C5E79A1015E4B9A3ACDB48B845845D9F4B5C7FDF4961000270AB8C2DAF 4
Malicious:	**true**
Reputation:	unknown
Preview:	1i.=..H

C:\Users\user\AppData\Roaming\ngneqippkv\anlq.exe	
Process:	C:\Users\user\Desktop\039846H0INVOICERECEIPT.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	635846
Entropy (8bit):	7.265896534672954
Encrypted:	false
SSDEEP:	12288:wkelR0/7/mpgcoDrMAJvRZ2/JPv5xEG44LV3M5VQTJ:Fyy/7EMnMAJZZqPRxEUhKY
MD5:	3BA78ED2E621B7BB47778EC2567DF223
SHA1:	D735536D9984DB49348E636D13CA0779D76B5D11
SHA-256:	329DEF14E6FA2AA0786DF6501894EFE890F27D250160397A16740A0BC731E967
SHA-512:	0C7B44ABD55C0EE3BEF28849D1C6660409489FBCC97635273E9E6F61D522529F374D5BD7266FB267B781A29CC863FF90C60CA98ACF13D216EFAC0A99A010038
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 33%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....Z.....%2.....p....@.....0.....s.....e.....p.....tex t...vY.....Z..... ..`.rdata.....p.....^.....@..@.data.....p.....@....ndata.....@.....rsrc....e.....f...t.....@..@..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.265896534672954

General

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:	039846H0INVOICERECEIPT.exe
File size:	635846
MD5:	3ba78ed2e621b7bb47778ec2567df223
SHA1:	d735536d9984db49348e636d13ca0779d76b5d11
SHA256:	329def14e6fa2aa0786df6501894efe890f27d250160397a16740a0bc731e967
SHA512:	0c7b44abd55c0ee3bef28849d1c6660409489fbcc97635273e9e6f61d522529f374d5bd7266fb267b781a29cc863ff90c60ca98acf13d216efac0a99a0100380
SSDEEP:	12288:wkelR0/7/mpgcoDrMAJvRZ2/JPv5xEG44LV3M5VQTJ:Fyy/7EMnMAJZZqPRxEUhKY
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:	844048d8e119cc10

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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x365a0	0x36600	False	0.536521192529	data	5.19064157442	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
01/12/22-18:38:14.752086	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	65447	8.8.8.8	192.168.2.5
01/12/22-18:38:21.213359	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52441	8.8.8.8	192.168.2.5
01/12/22-18:38:26.409181	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59596	8.8.8.8	192.168.2.5
01/12/22-18:38:44.795475	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56969	8.8.8.8	192.168.2.5
01/12/22-18:38:50.028428	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55161	8.8.8.8	192.168.2.5
01/12/22-18:38:55.291504	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55016	8.8.8.8	192.168.2.5
01/12/22-18:39:08.058603	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50463	8.8.8.8	192.168.2.5
01/12/22-18:39:13.357094	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50394	8.8.8.8	192.168.2.5
01/12/22-18:39:28.259863	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56432	8.8.8.8	192.168.2.5
01/12/22-18:40:07.983394	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57172	8.8.8.8	192.168.2.5

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 12, 2022 18:38:14.636555910 CET	192.168.2.5	8.8.8.8	0xe10	Standard query (0)	girlhomejan6100.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:38:21.100702047 CET	192.168.2.5	8.8.8.8	0xe10f	Standard query (0)	girlhomejan6100.duckdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:38:26.296413898 CET	192.168.2.5	8.8.8.8	0x4f81	Standard query (0)	girlhomejan6100.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 12, 2022 18:38:31.649983883 CET	192.168.2.5	8.8.8.8	0x5307	Standard query (0)	girlhomeja n6100.duck dns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:38:39.037731886 CET	192.168.2.5	8.8.8.8	0xd737	Standard query (0)	girlhomeja n6100.duck dns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:38:44.682404995 CET	192.168.2.5	8.8.8.8	0x9023	Standard query (0)	girlhomeja n6100.duck dns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:38:49.917918921 CET	192.168.2.5	8.8.8.8	0xf926	Standard query (0)	girlhomeja n6100.duck dns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:38:55.178416967 CET	192.168.2.5	8.8.8.8	0xb6e9	Standard query (0)	girlhomeja n6100.duck dns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:02.680068970 CET	192.168.2.5	8.8.8.8	0x4416	Standard query (0)	girlhomeja n6100.duck dns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:07.945353985 CET	192.168.2.5	8.8.8.8	0x6b6c	Standard query (0)	girlhomeja n6100.duck dns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:13.246021032 CET	192.168.2.5	8.8.8.8	0x81b	Standard query (0)	girlhomeja n6100.duck dns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:21.608736038 CET	192.168.2.5	8.8.8.8	0xb29a	Standard query (0)	girlhomeja n6100.duck dns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:28.146733046 CET	192.168.2.5	8.8.8.8	0xdb3c	Standard query (0)	girlhomeja n6100.duck dns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:35.464998007 CET	192.168.2.5	8.8.8.8	0x53dd	Standard query (0)	girlhomeja n6100.duck dns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:42.102267027 CET	192.168.2.5	8.8.8.8	0x3909	Standard query (0)	girlhomeja n6100.duck dns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:48.673012972 CET	192.168.2.5	8.8.8.8	0x3282	Standard query (0)	girlhomeja n6100.duck dns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:55.341304064 CET	192.168.2.5	8.8.8.8	0x50e3	Standard query (0)	girlhomeja n6100.duck dns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:40:01.727452993 CET	192.168.2.5	8.8.8.8	0xcb4a	Standard query (0)	girlhomeja n6100.duck dns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 18:40:07.870163918 CET	192.168.2.5	8.8.8.8	0xbd93	Standard query (0)	girlhomeja n6100.duck dns.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 18:38:14.752085924 CET	8.8.8.8	192.168.2.5	0xe10	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:38:21.213359118 CET	8.8.8.8	192.168.2.5	0xe10f	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:38:26.409181118 CET	8.8.8.8	192.168.2.5	0x4f81	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:38:31.668584108 CET	8.8.8.8	192.168.2.5	0x5307	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:38:39.056185007 CET	8.8.8.8	192.168.2.5	0xd737	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:38:44.795475006 CET	8.8.8.8	192.168.2.5	0x9023	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:38:50.028428078 CET	8.8.8.8	192.168.2.5	0xf926	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:38:55.291503906 CET	8.8.8.8	192.168.2.5	0xb6e9	No error (0)	girlhomeja n6100.duck dns.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 18:39:02.699554920 CET	8.8.8.8	192.168.2.5	0x4416	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:08.058603048 CET	8.8.8.8	192.168.2.5	0x6b6c	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:13.357094049 CET	8.8.8.8	192.168.2.5	0x81b	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:21.625154972 CET	8.8.8.8	192.168.2.5	0xb29a	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:28.259862900 CET	8.8.8.8	192.168.2.5	0xdb3c	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:35.483736992 CET	8.8.8.8	192.168.2.5	0x53dd	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:42.118866920 CET	8.8.8.8	192.168.2.5	0x3909	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:48.692035913 CET	8.8.8.8	192.168.2.5	0x3282	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:39:55.361430883 CET	8.8.8.8	192.168.2.5	0x50e3	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:40:01.744152069 CET	8.8.8.8	192.168.2.5	0xcb4a	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)
Jan 12, 2022 18:40:07.983393908 CET	8.8.8.8	192.168.2.5	0xbd93	No error (0)	girlhomeja n6100.duck dns.org		194.5.98.28	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 039846H0INVOICERECEIPT.exe PID: 5220 Parent PID: 5212

General

Start time:	18:38:03
Start date:	12/01/2022
Path:	C:\Users\user\Desktop\039846H0INVOICERECEIPT.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\039846H0INVOICERECEIPT.exe"
Imagebase:	0x400000
File size:	635846 bytes
MD5 hash:	3BA78ED2E621B7BB47778EC2567DF223
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: 00000000.00000002.249043381.00000000031A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.249043381.00000000031A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.249043381.00000000031A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.249043381.00000000031A0000.00000004.00000001.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: 039846H0INVOICERECEIPT.exe PID: 4396 Parent PID: 5220

General

Start time:	18:38:05
Start date:	12/01/2022
Path:	C:\Users\user\Desktop\039846H0INVOICERECEIPT.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\039846H0INVOICERECEIPT.exe"
Imagebase:	0x400000
File size:	635846 bytes
MD5 hash:	3BA78ED2E621B7BB47778EC2567DF223
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.508293325.0000000003904000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.508293325.0000000003904000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000000.246308898.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000000.246308898.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000000.246308898.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.508341763.0000000003962000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.503636006.00000000024E2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.503636006.00000000024E2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.503636006.00000000024E2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.498126981.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.498126981.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.498126981.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.498126981.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.498719213.0000000000675000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.498719213.0000000000675000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.498719213.0000000000675000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.507080103.0000000002924000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.503483350.00000000024A0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.503483350.00000000024A0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.503483350.00000000024A0000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.503483350.00000000024A0000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000000.244362493.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000000.244362493.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000000.244362493.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.507854463.0000000002A81000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.504358313.00000000028D1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: anlq.exe PID: 3224 Parent PID: 3472

General

Start time:	18:38:17
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:	635846 bytes
MD5 hash:	3BA78ED2E621B7BB47778EC2567DF223
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: 00000005.00000002.279178171.0000000003160000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.279178171.0000000003160000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.279178171.0000000003160000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.279178171.0000000003160000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 33%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: anlq.exe PID: 6196 Parent PID: 3224

General

Start time:	18:38:21
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:	635846 bytes
MD5 hash:	3BA78ED2E621B7BB47778EC2567DF223
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000007.00000002.292734330.000000000277E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.275663964.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.275663964.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.275663964.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.292594850.00000000022E2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.292594850.00000000022E2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.292594850.00000000022E2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.292082066.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.292082066.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.292082066.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.292082066.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.292219672.0000000000624000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.292219672.0000000000624000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.292219672.0000000000624000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.292806006.0000000003771000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.292806006.0000000003771000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.292806006.0000000003771000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000001.277541562.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000001.277541562.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000001.277541562.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000001.277541562.0000000000400000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.292556739.00000000022A0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.292556739.00000000022A0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.292556739.00000000022A0000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.292556739.00000000022A0000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.276749512.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.276749512.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.276749512.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.292893122.00000000037AA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.292893122.00000000037AA000.00000004.00000001.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: 6332 Parent PID: 3472

General

Start time:	18:38:25
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:	635846 bytes
MD5 hash:	3BA78ED2E621B7BB47778EC2567DF223
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: 00000009.00000002.297921153.0000000002470000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.297921153.0000000002470000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.297921153.0000000002470000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.297921153.0000000002470000.00000004.00000001.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: 6392 Parent PID: 6332

General

Start time:	18:38:27
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:	635846 bytes
MD5 hash:	3BA78ED2E621B7BB47778EC2567DF223

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: 0000000B.00000000.294082200.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.294082200.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.294082200.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.313908924.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.313908924.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.313908924.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.313908924.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.314341475.0000000002610000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.314341475.0000000002610000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.314341475.0000000002610000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.314341475.0000000002610000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.314490678.0000000002A5E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.314014470.0000000000504000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.314014470.0000000000504000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.314014470.0000000000504000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.314375073.0000000002652000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.314375073.0000000002652000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.314375073.0000000002652000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.296175339.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.296175339.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.296175339.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.314547545.0000000003A8A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.314547545.0000000003A8A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.314517163.0000000003A51000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.314517163.0000000003A51000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.314517163.0000000003A51000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis