ID: 558450
Sample Name: INQUIRY.exe
Cookbook: default.jbs
Time: 02:23:21
Date: 24/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

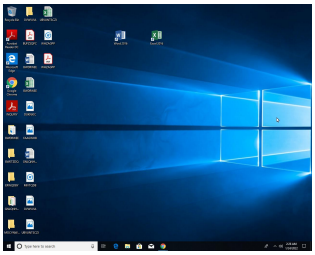
Windows Analysis Report

INQUIRY.exe

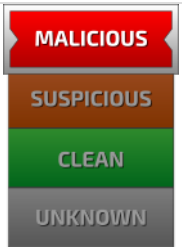
Overview

General Information

Sample Name:	INQUIRY.exe
Analysis ID:	558450
MD5:	dc0acc75361bb3..
SHA1:	9e9c823725bee1..
SHA256:	d73cbcb2d300d8..
Infos:	



Detection



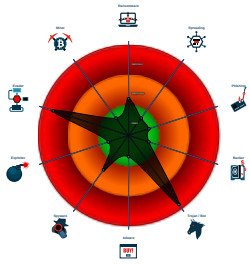
Nanocore

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Yara detected Nanocore RAT
- Detected unpacking (creates a PE f…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Found evasive API chain (may stop…
- Machine Learning detection for drop…

Classification



Process Tree

- **System is w10x64**
- INQUIRY.exe (PID: 6904 cmdline: "C:\Users\user\Desktop\INQUIRY.exe" MD5: DC0ACC75361BB39FBD4ABEC6EDC82CD5)
  - INQUIRY.exe (PID: 7084 cmdline: "C:\Users\user\Desktop\INQUIRY.exe" MD5: DC0ACC75361BB39FBD4ABEC6EDC82CD5)
- rstmgknbahw.exe (PID: 6472 cmdline: "C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe" MD5: DC0ACC75361BB39FBD4ABEC6EDC82CD5)
  - rstmgknbahw.exe (PID: 1904 cmdline: "C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe" MD5: DC0ACC75361BB39FBD4ABEC6EDC82CD5)
- rstmgknbahw.exe (PID: 4296 cmdline: "C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe" MD5: DC0ACC75361BB39FBD4ABEC6EDC82CD5)
  - rstmgknbahw.exe (PID: 5320 cmdline: "C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe" MD5: DC0ACC75361BB39FBD4ABEC6EDC82CD5)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "b46b5964-4830-4c6b-9df5-a21557a1",
  "Group": "Default",
  "Domain1": "onyeoma.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 4141,
  "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
00000005.00000002.719731750.0000000002400000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x215e5:$x1: NanoCore.ClientPluginHost • 0x21622:$x2: IClientNetworkHost • 0x25155:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000005.00000002.719731750.0000000002400000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2135d:$x1: NanoCore Client.exe • 0x215e5:$x2: NanoCore.ClientPluginHost • 0x22c1e:$s1: PluginCommand • 0x22c12:$s2: FileCommand • 0x23ac3:$s3: PipeExists • 0x2987a:$s4: PipeCreated • 0x2160f:$s5: IClientLoggingHost
00000005.00000002.719731750.0000000002400000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000005.00000002.719731750.0000000002400000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2134d:$a: NanoCore • 0x2135d:$a: NanoCore • 0x21591:$a: NanoCore • 0x215a5:$a: NanoCore • 0x215e5:$a: NanoCore • 0x213ac:$b: ClientPlugin • 0x215ae:$b: ClientPlugin • 0x215ee:$b: ClientPlugin • 0x214d3:$c: ProjectData • 0x21eda:$d: DESCrypto • 0x298a6:$e: KeepAlive • 0x27894:$g: LogClientMessage • 0x23a8f:$i: get_Connected • 0x22210:$j: #=q • 0x22240:$j: #=q • 0x2225c:$j: #=q • 0x2228c:$j: #=q • 0x222a8:$j: #=q • 0x222c4:$j: #=q • 0x222f4:$j: #=q • 0x22310:$j: #=q
00000002.00000000.662575253.0000000000414000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x111e5:$x1: NanoCore.ClientPluginHost • 0x11222:$x2: IClientNetworkHost • 0x14d55:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Click to see the 99 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.rstmgknbahw.exe.400000.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x85e5:$x1: NanoCore.ClientPluginHost • 0x8622:$x2: IClientNetworkHost • 0xc155:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
6.0.rstmgknbahw.exe.400000.1.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x835d:$x1: NanoCore Client.exe • 0x85e5:$x2: NanoCore.ClientPluginHost • 0x9c1e:$s1: PluginCommand • 0x9c12:$s2: FileCommand • 0xaac3:$s3: PipeExists • 0x1087a:$s4: PipeCreated • 0x860f:$s5: IClientLoggingHost
6.0.rstmgknbahw.exe.400000.1.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
6.0.rstmgknbahw.exe.400000.1.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x834d:$a: NanoCore • 0x835d:$a: NanoCore • 0x8591:$a: NanoCore • 0x85a5:$a: NanoCore • 0x85e5:$a: NanoCore • 0x83ac:$b: ClientPlugin • 0x85ae:$b: ClientPlugin • 0x85ee:$b: ClientPlugin • 0x84d3:$c: ProjectData • 0x8eda:$d: DESCrypto • 0x108a6:$e: KeepAlive • 0xe894:$g: LogClientMessage • 0xaa8f:$i: get_Connected • 0x9210:$j: #=q • 0x9240:$j: #=q • 0x925c:$j: #=q • 0x928c:$j: #=q • 0x92a8:$j: #=q • 0x92c4:$j: #=q • 0x92f4:$j: #=q • 0x9310:$j: #=q
6.2.rstmgknbahw.exe.37a3258.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 416 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

AV Detection

Found malware configuration

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

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

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)

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)

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

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

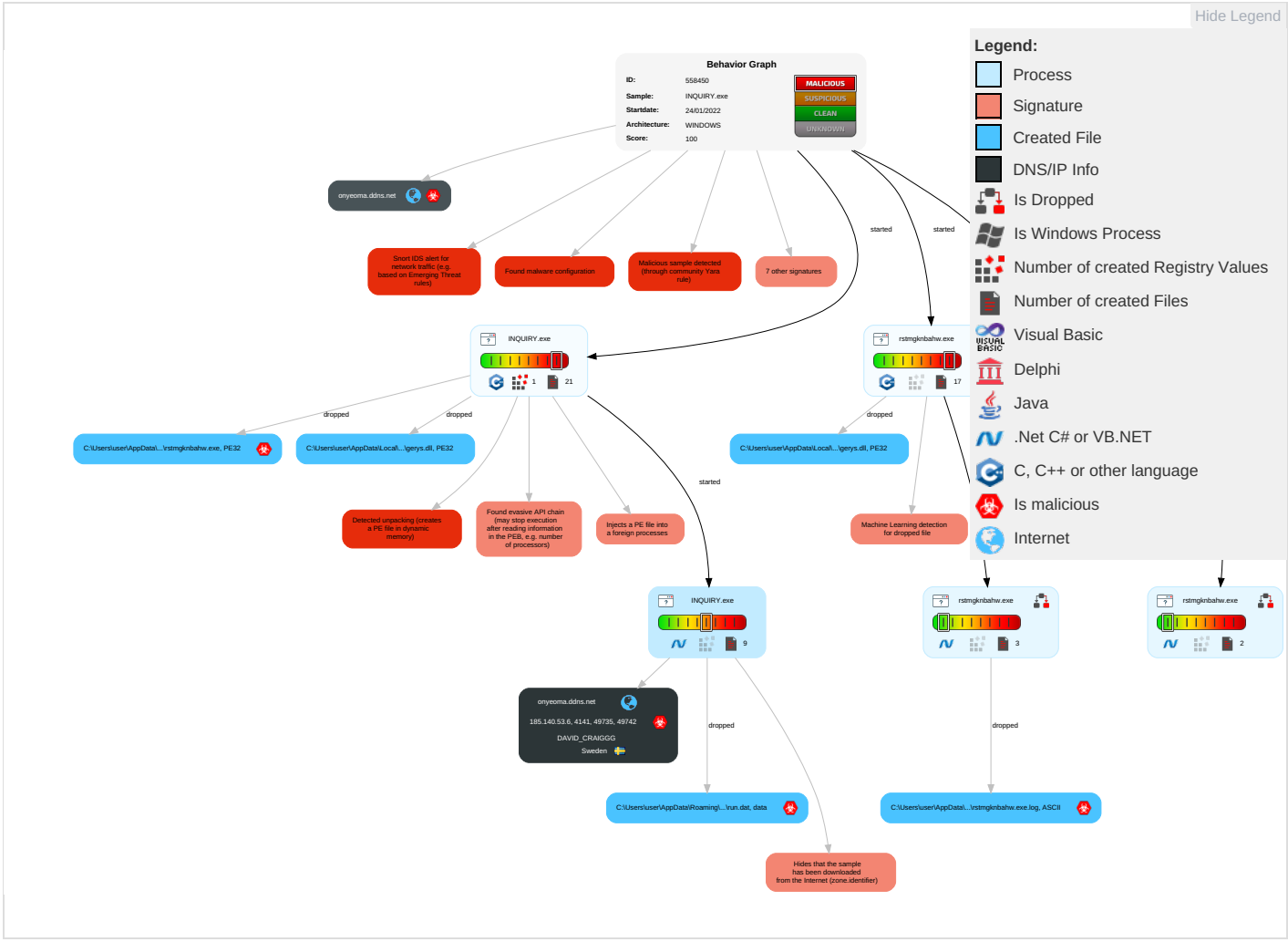
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Native API	1 Registry Run Keys / Startup Folder	1 1 2 Process Injection	1 Disable or Modify Tools	1 1 Input Capture	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 1 Input Capture	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	1 5 System Information Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 1 Software Packing	NTDS	2 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	2 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 2 Process Injection	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

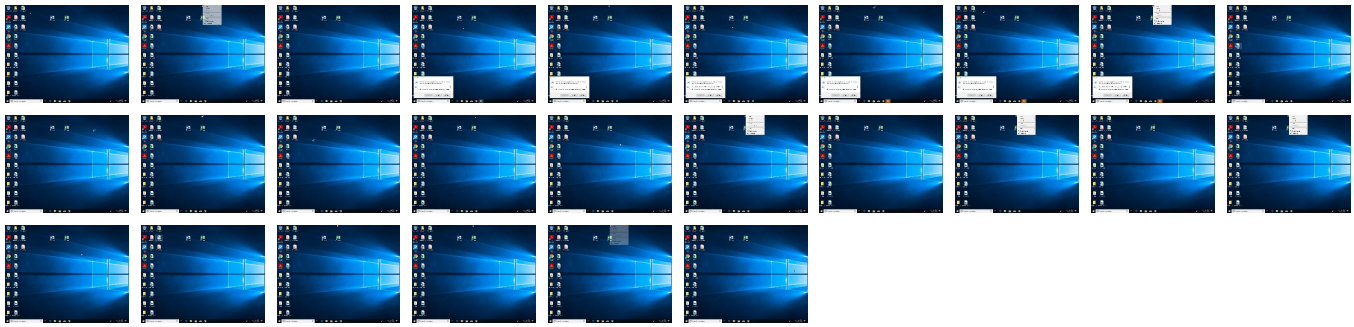
Behavior Graph



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
INQUIRY.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.rstmgknbahw.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.2.INQUIRY.exe.30e0000.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.INQUIRY.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.0.INQUIRY.exe.400000.7.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.0.rstmgknbahw.exe.400000.7.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.0.INQUIRY.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
6.2.rstmgknbahw.exe.4980000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.0.rstmgknbahw.exe.400000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.rstmgknbahw.exe.49d0000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.rstmgknbahw.exe.400000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.0.INQUIRY.exe.400000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.0.INQUIRY.exe.400000.11.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.0.rstmgknbahw.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.2.rstmgknbahw.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.1.rstmgknbahw.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.0.rstmgknbahw.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.rstmgknbahw.exe.400000.11.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.rstmgknbahw.exe.400000.7.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.rstmgknbahw.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.1.rstmgknbahw.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.INQUIRY.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.INQUIRY.exe.39a98c0.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
6.0.rstmgknbahw.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.rstmgknbahw.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.0.rstmgknbahw.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.INQUIRY.exe.2520000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.rstmgknbahw.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.0.INQUIRY.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.0.INQUIRY.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.0.rstmgknbahw.exe.400000.11.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.rstmgknbahw.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
onyeoma.ddns.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
onyeoma.ddns.net	0%	Virustotal		Browse
onyeoma.ddns.net	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Virustotal		Browse
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
onyeoma.ddns.net	185.140.53.6	true	true	• 0%, Virustotal, Browse	unknown

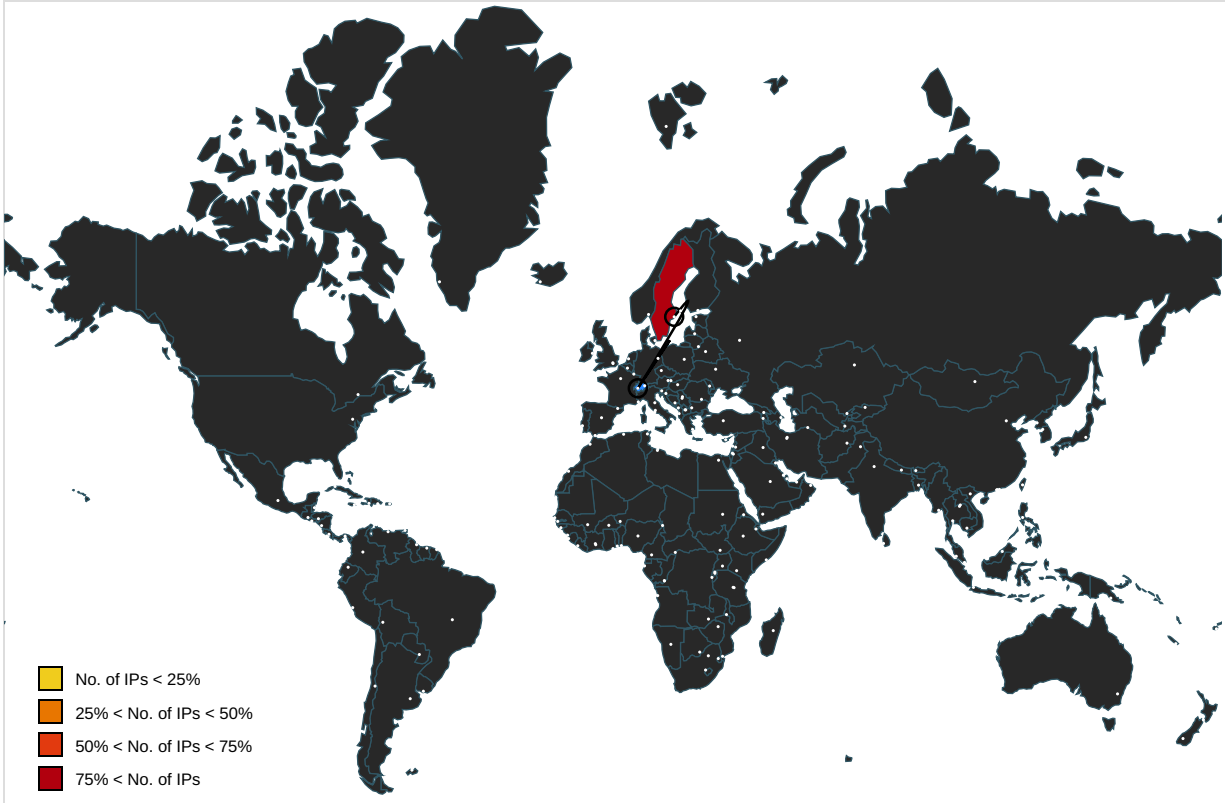
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
onyeoma.ddns.net	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
127.0.0.1	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_Error	rstmgknbahw.exe, rstmgknbahw.exe, 00000005.00000002.719289522.0000000000409000.00000004.00020000.sdmp, rstmgknbahw.exe, 00000005.00000000.695461777.0000000000409000.00000008.00020000.sdmp, rstmgknbahw.exe, 00000006.00000000.707759536.0000000000409000.00000008.00020000.sdmp, INQUIRY.exe, rstmgknbahw.exe.1.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	INQUIRY.exe, rstmgknbahw.exe.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.6	onyeoma.ddns.net	Sweden		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	558450
Start date:	24.01.2022
Start time:	02:23:21

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INQUIRY.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:	21
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: 83.3%
HDC Information:	• Successful, ratio: 71.6% (good quality ratio 66.4%) • Quality average: 75.8% • Quality standard deviation: 31.1%
HCA Information:	• Successful, ratio: 85% • 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

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, store-images.s-microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target INQUIRY.exe, PID 7084 because there are no executed function
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
02:24:15	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run earyw C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe
02:24:18	API Interceptor	962x Sleep call for process: INQUIRY.exe modified
02:24:23	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run earyw C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe
02:24:29	API Interceptor	2x Sleep call for process: rstmgknbahw.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\rstmgknbahw.exe.log

Process:	C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.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:	high, very likely benign file
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\m30xh3rgrf9sf7w0k

Process:	C:\Users\user\Desktop\INQUIRY.exe
File Type:	data
Category:	dropped
Size (bytes):	278527
Entropy (8bit):	7.986066778609259
Encrypted:	false
SSDEEP:	6144:TYEMx0q3EXCouk+eWWP1QbXva183aCT0B/ER78PemFd/1X:TYxZ3Q8Heldu4IaCTm/HX59
MD5:	16FC364F28AB0F84C023E255CE6B0793
SHA1:	BD610A8C17B0A5C0C0AF67542F7533271229F584
SHA-256:	167379B6A1CD5727CCA9F6891B4A58FF06C42490E61D7AE7F8AAFD26F05D1B38
SHA-512:	D042B54CA997370F3B86FF5567D956489FF7FF9EED92CF5822FE6CDCDB1FB88EC37011E2F6D498BFBD6811CF6C668C0DADD68FFE58642C6B82842B32E2AA75CC
Malicious:	false
Reputation:	low
Preview:	..8..'.....".8.`.;Z.t.~.....R._..![...j9B..[f.E$<R&.(.=...P..*{m..-.]..G.#..'...D.)...~`..."...{.0...5U.L.L....?A.p.5.3tw....6...\|VW.u$..\..7.....v..tTK..<?..cf..:..-..2..g.....j.].A....n.~..Ne-.#='..#.....5fGeG..k...6.5~A.3.|Y.C+...&..YF..'..^..R..8...Z.t.....k.._.![...j9B.U.f.E.<R&.(...V..t..{....(}.\Wbf.J....w.....s.....$.Dxy.G.0.K.Cp.5V3tw.~z...[.a..@.\|.{..!.G[....$.s|...dRg-Q....._.....w..u).....2.\.8sw.=..E.L..g...y.v....f.u.....j....$Wv.(IS.....C+...&.j.pN.'.....!.8.J.;Z.t.....R....y./g.i$B.2zf.E.<R&.(.."......{2...(..|Wb..Z...w....I.....s.Xc....$.9xy.G*0.6K...UO..tw.~z..#..Y0%@h..{.#.....$.!|.=.[|JQ..J..j..{.w.....u).....\k8sw.=..6....g...y.v....fTu.....j....$Wv.(IS.....C+...&..YF..'.....M.8.`.;Z.t.....R._..![...j9B..[f.E$<R&.(.....{2...(..\Wbf.Jo...w.....s.....$.9xy.G*0.6K.Cp.5.3tw.~z...[.Y.%@h\|.{.#.....$.s|...dRg-Q....._..{r...w..u).....2.\.8sw.=..6....g...y.v....fTu.....

C:\Users\user\AppData\Local\Temp\nsc48D5.tmp

Process:	C:\Users\user\Desktop\INQUIRY.exe
File Type:	data
Category:	dropped
Size (bytes):	328199
Entropy (8bit):	7.763501353201283
Encrypted:	false
SSDEEP:	6144:KU0YEMx0q3EXCouk+eWWP1QbXva183aCT0B/ER78PemFd/1OF2:QYxZ3Q8Heldu4IaCTm/HX5q2
MD5:	6EB0F8E8E159CC6BE6F7C45CA7B714F2
SHA1:	85A286A84D5344F29261BAC2622C98F61DC3BC6A
SHA-256:	F85D1A62A230E16ACCF48069072C12F4EDD62350375FF21AF97257AC90CF8874
SHA-512:	D6D0EA566DC37B961F2A16BF6BC892B261B92183C3BDB709F2B895E2BBA6E3E8DE1AD4A7D99767ECEA5890A364FA759DFD7E3C274F4B2080BBF9C3624A668544
Malicious:	false
Reputation:	low
Preview:	.\.....,.....F...lE.....[.....m\.....J.....#...j.....$..........

C:\Users\user\AppData\Local\Temp\nsc48D6.tmp\gerys.dll

Process:	C:\Users\user\Desktop\INQUIRY.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18432
Entropy (8bit):	5.728423253996569
Encrypted:	false
SSDEEP:	384:fWrH9a+IIcHqWIHcJALBQNdZCvSdQkU7kO0Kkqb:0nlIfWILoLUSdQHkJKT
MD5:	964F57C518C022C62A555DEB4E48D02E
SHA1:	B71006B1850415DDF27B656A18382963EDBD4C9D
SHA-256:	DAAEED4ABBDCB59F82CB65AC2C32929E52E821E9068A2B453ABD3118DF1E9378
SHA-512:	296D4B41119F294E4D86B7CA5EE395C05F3AD9520B98391DACD34AECCCB733092DB7134CBA935863D5E45235C593171B71D8507292AD44E6B9FE8BD6BF5C200
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...0...0...0...[...0...0...0..Ln...0..Ln...0..In...0..Ln...0..Rich.0.....PE..L.....a.....!.....8.....P.....@.....P..H...8Q.....`.....p..p.....P.....text....6.....8..... .`.rdata..&....P.....<.....@..@.rsrc.....`.....D.....@..@.reloc..p....p.....F.....@..B.....

C:\Users\user\AppData\Local\Temp\nsv9D9C.tmp

Process:	C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe
File Type:	data
Category:	dropped
Size (bytes):	328199
Entropy (8bit):	7.763501353201283
Encrypted:	false
SSDEEP:	6144:KU0YEMx0q3EXCouk+eWWP1QbXva183aCT0B/ER78PemFd/1OF2:QYxZ3Q8Heldu4IaCTm/HX5q2
MD5:	6EB0F8E8E159CC6BE6F7C45CA7B714F2
SHA1:	85A286A84D5344F29261BAC2622C98F61DC3BC6A
SHA-256:	F85D1A62A230E16ACCF48069072C12F4EDD62350375FF21AF97257AC90CF8874
SHA-512:	D6D0EA566DC37B961F2A16BF6BC892B261B92183C3BDB709F2B895E2BBA6E3E8DE1AD4A7D99767ECEA5890A364FA759DFD7E3C274F4B2080BBF9C3624A668544
Malicious:	false
Reputation:	low
Preview:	.\.....,.....F...lE.....[.....m\.....J.....#...j.....$..........

C:\Users\user\AppData\Local\Temp\nsv9D9D.tmp\gerys.dll

Process:	C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	18432
Entropy (8bit):	5.728423253996569
Encrypted:	false
SSDEEP:	384:fWrH9a+IIcHqWIHcJALBQNdZCvSdQkU7kO0Kkqb:0nIIfWILoLUSdQHkJKT
MD5:	964F57C518C022C62A555DEB4E48D02E
SHA1:	B71006B1850415DDF27B656A18382963EDBD4C9D
SHA-256:	DAAEED4ABBDCB59F82CB65AC2C32929E52E821E9068A2B453ABD3118DF1E9378
SHA-512:	296D4B41119F294E4D86B7CA5EE395C05F3AD9520B98391DACD34AECCCB733092DB7134CBA935863D5E45235C593171B71D8507292AD44E6B9FE8BD6BF5C20 0
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...0...0...0...[...0...0...0..Ln...0..Ln...0..In...0..Ln...0..Rich.0..... .....PE..L.....a.....!....8.....P.....@.....P..H...8Q.....`.....p..p.....P..... .....text....6.....8..... ..`.rdata..&....P.....<.....@..@.rsrc.....`.....D.....@..@.reloc..p....p.....F.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsz814A.tmp

Process:	C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe
File Type:	data
Category:	dropped
Size (bytes):	328199
Entropy (8bit):	7.763501353201283
Encrypted:	false
SSDEEP:	6144:KU0YEMx0q3EXCouk+eWWP1QbXva183aCT0B/ER78PemFd/1OF2:QYxZ3Q8Heldu4IaCTm/HX5q2
MD5:	6EB0F8E8E159CC6BE6F7C45CA7B714F2
SHA1:	85A286A84D5344F29261BAC2622C98F61DC3BC6A
SHA-256:	F85D1A62A230E16ACCF48069072C12F4EDD62350375FF21AF97257AC90CF8874
SHA-512:	D6D0EA566DC37B961F2A16BF6BC892B261B92183C3BDB709F2B895E2BBA6E3E8DE1AD4A7D99767ECEA5890A364FA759DFD7E3C274F4B2080BBF9C3624A668 44
Malicious:	false
Reputation:	low
Preview:	.\.....,.....F...lE.....[.....m\..... .....J.....#...j.....$..... ....

C:\Users\user\AppData\Local\Temp\nsz814B.tmp\gerys.dll

Process:	C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18432
Entropy (8bit):	5.728423253996569
Encrypted:	false
SSDEEP:	384:fWrH9a+IIcHqWIHcJALBQNdZCvSdQkU7kO0Kkqb:0nIIfWILoLUSdQHkJKT
MD5:	964F57C518C022C62A555DEB4E48D02E
SHA1:	B71006B1850415DDF27B656A18382963EDBD4C9D
SHA-256:	DAAEED4ABBDCB59F82CB65AC2C32929E52E821E9068A2B453ABD3118DF1E9378
SHA-512:	296D4B41119F294E4D86B7CA5EE395C05F3AD9520B98391DACD34AECCCB733092DB7134CBA935863D5E45235C593171B71D8507292AD44E6B9FE8BD6BF5C20 0
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...0...0...0...[...0...0...0..Ln...0..Ln...0..In...0..Ln...0..Rich.0..... .....PE..L.....a.....!....8.....P.....@.....P..H...8Q.....`.....p..p.....P..... .....text....6.....8..... ..`.rdata..&....P.....<.....@..@.rsrc.....`.....D.....@..@.reloc..p....p.....F.....@..B..... ....

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

Process:	C:\Users\user\Desktop\INQUIRY.exe
File Type:	data
Category:	dropped

Size (bytes):	7539
Entropy (8bit):	6.073593928396658
Encrypted:	false
SSDEEP:	192:dCBXlCcDOOqcG8KiqmpLiu90E6lJu96utIdlxaP:4trDOOqcGce807u0u2fxy
MD5:	7AA8D1B3501B957F963AD8B0E873510C
SHA1:	8DF70D69A3B89166FAF60D2E8BB0F2BADBA9CB10
SHA-256:	350C38CCDE959E201754E7469F8149A7548A789160B202CF6397AAF439987638
SHA-512:	0926C416DA709AE8ECB6C79A300BB2692A80541C183859C959F292B4E9201DB8937CD2E5D757318FD60311B1F1D77C3B0C93E5330BC82A5A89D0F477BE7E687
Malicious:	false
Reputation:	low
Preview:	..qtt.....tl.4.IE..I.4.IE.....t1..Lttt...t9_h9_D....ttt.....9_h9_D....ttt.....9_h9_D....ttt.....9_h9_D....ttt.,..(9_h9_D....ttt.4..0.WDpb..l|.4uu.h.....D..p%+.....p3%..D{....u...p6.....%.tttt.pPo-M..9_.{9_.~9_,.|9_4.{9_.Y9_.z..`D...h...T..s_.9_..~.llo..u...tttt1.PpUttt.pPg-..zY..Yz}..w6ht.....I.4.IE...l.t..heT.l.t.D.@3....3p...l.t..l.s.....w6ht.B.2..\vtt..vtt6@t..9...vtt.xvtt6lt.gx....vt t..vtt6lt.....LI.4.IE..1..Dttt.....W.t`B..2tt.....@ott.4`..l..l{.+t.g..g.....l{3.t.g..g..v.l|.4t.o....9...stt..*.99...l...9_l..999...W.t`r...t.q1..sttt....w6pt.....I.4.IE..1..Lttt.4...W.t`B..2tt.....  ...ptt.4I..ttt.l..l{.+t.g4.g0.h..l{3.t.g4.g0.D..l{...g4.g0.@%+.l~..u.?4.?0....l{3.v.g4.g0.o.l|.4t.o4..B.2...ttt....99...W<t`l...<.s.A9_<9_@9_D9_h9_l.!.99...W.t`r...t.q1..sttt....w6 @t.....81..Dttt.....W.t`B..2tt.....utt.4`..l..l{.+t.g..g..h..l{3.t.g..g..v.l|.4t.o...gx...Qttt..P.99...j9_

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

Process:	C:\Users\user\Desktop\INQUIRY.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
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF3851
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... 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\INQUIRY.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:3e8t:B
MD5:	CF0C25BF3DC4FFBB8F3E0CDC145DD33E
SHA1:	6ED58B87F71DA1F789EB1A81A6FB08C314FB508A
SHA-256:	34B778FCE744D50ADF7F57F7CA5480538294B496E425C141ED07EBC5A17CB81F
SHA-512:	D22752D21943BD8DBF30B48066B1F8DCDB139467D4352A7E114DBBBE4EB082F8A3566F0865DE93B138FDAC5FEE83D673C32D727B864419572C382EFBA8D9608
Malicious:	**true**
Preview:	k=.>...H

C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe

Process:	C:\Users\user\Desktop\INQUIRY.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	315125
Entropy (8bit):	7.883283847039061
Encrypted:	false
SSDEEP:	6144:/w8yH0o3Hx8NFIImn7/q7cly7x5rYFggsIKW4BSusOM0odo5BehhFl7/:W0vII073lMhYOsKPBSusOWo5Al7/
MD5:	DC0ACC75361BB39FBD4ABEC6EDC82CD5
SHA1:	9E9C823725BEE12D0980009C04692AD9089D9308
SHA-256:	D73CBCB2D300D84618D476706765B185C12D20D2E52AFE120FB587C81BE7CC80

SHA-512:	F40CB60C1D80B09322783BFC83C34784CD28F9B6462701AA069C867986DF99DB06CB088203B02D6F6CA8CCB95FF60AE856D8B92FC2D40BC64E1134EB950CC96
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....p....@.....s.....HA.....p.....text...vY.....Z..... ..`.rdata.....p.....^.....@..@.data.....p.....@....ndata.....@.....rsrc...HA.....B...t.....@..@.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.883283847039061
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:	INQUIRY.exe
File size:	315125
MD5:	dc0acc75361bb39fbd4abec6edc82cd5
SHA1:	9e9c823725bee12d0980009c04692ad9089d9308
SHA256:	d73cbcb2d300d84618d476706765b185c12d20d2e52afe120fb587c81be7cc80
SHA512:	f40cb60c1d80b09322783bfc83c34784cd28f9b6462701aa069c867986df99db06cb088203b02d6f6ca8ccb95ff60ae856d8b92fc2d40bc64e1134eb950cc996
SSDEEP:	6144:/w8yH0o3Hx8NFIImn7/q7cly7x5rYFggsIKW4BSusOM0odo5BehhFl7/:W0vII073lMhYOsKPBSusOWo5Al7/
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:	0c129232d9ccc41b

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

Instruction
sub esp, 00000180h
push ebx

Instruction
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409128h
xor esi, esi
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407030h]
push 00008001h
call dword ptr [004070B4h]
push ebx
call dword ptr [0040727Ch]
push 00000008h
mov dword ptr [00423F58h], eax
call 00007F9F28CAD860h
mov dword ptr [00423EA4h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F450h
call dword ptr [00407158h]
push 004091B0h
push 004236A0h
call 00007F9F28CAD517h
call dword ptr [004070B0h]
mov edi, 00429000h
push eax
push edi
call 00007F9F28CAD505h
push ebx
call dword ptr [0040710Ch]
cmp byte ptr [00429000h], 00000022h
mov dword ptr [00423EA0h], eax
mov eax, edi
jne 00007F9F28CAAD2Ch
mov byte ptr [esp+14h], 00000022h
mov eax, 00429001h
push dword ptr [esp+14h]
push eax
call 00007F9F28CACFF8h
push eax
call dword ptr [0040721Ch]
mov dword ptr [esp+1Ch], eax
jmp 00007F9F28CAAD85h
cmp cl, 00000020h
jne 00007F9F28CAAD28h
inc eax
cmp byte ptr [eax], 00000020h
je 00007F9F28CAAD1Ch
cmp byte ptr [eax], 00000022h
mov byte ptr [eax+eax+00h], 00000000h

Rich Headers	
Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x73a4	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x4148	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x28c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

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	0x4148	0x4200	False	0.209753787879	data	3.76510054969	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2c1f0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4289923840, next used block 4289923840	English	United States
RT_ICON	0x2e798	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4289923840, next used block 4289923840	English	United States
RT_ICON	0x2f840	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x2fca8	0x100	data	English	United States
RT_DIALOG	0x2fda8	0x11c	data	English	United States
RT_DIALOG	0x2fec8	0x60	data	English	United States
RT_GROUP_ICON	0x2ff28	0x30	data	English	United States
RT_MANIFEST	0x2ff58	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetTickCount, CreateFileA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, SetFileTime, GetTempPathA, GetCommandLineA, SetErrorMode, LoadLibraryA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, GetVersion, CloseHandle, lstrcmpiA, lstrcmpA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, GetModuleHandleA, LoadLibraryExA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, GetWindowsDirectoryA

DLL	Import
USER32.dll	EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, DestroyWindow, CreateDialogParamA, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, OpenClipboard, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

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

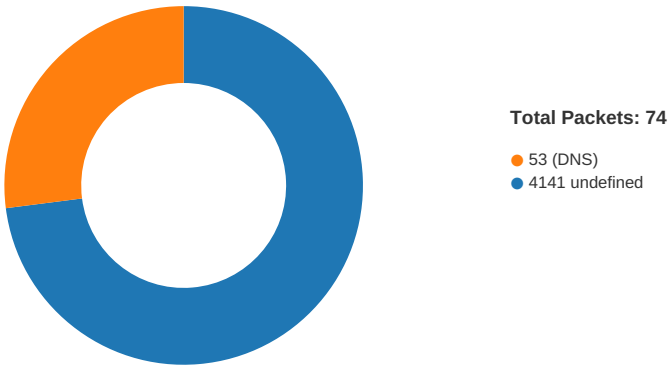
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/24/22-02:24:20.152195	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59123	8.8.8.8	192.168.2.4
01/24/22-02:24:20.743770	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	4141	192.168.2.4	185.140.53.6
01/24/22-02:24:26.623926	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54531	8.8.8.8	192.168.2.4
01/24/22-02:24:26.701611	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	4141	192.168.2.4	185.140.53.6
01/24/22-02:24:31.333067	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	4141	192.168.2.4	185.140.53.6
01/24/22-02:24:37.493200	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	4141	192.168.2.4	185.140.53.6
01/24/22-02:24:43.325751	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53097	8.8.8.8	192.168.2.4
01/24/22-02:24:43.429089	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	4141	192.168.2.4	185.140.53.6
01/24/22-02:24:50.367349	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62389	8.8.8.8	192.168.2.4
01/24/22-02:24:50.487020	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49760	4141	192.168.2.4	185.140.53.6
01/24/22-02:24:56.459195	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49767	4141	192.168.2.4	185.140.53.6
01/24/22-02:25:02.430704	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55854	8.8.8.8	192.168.2.4
01/24/22-02:25:02.524995	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49774	4141	192.168.2.4	185.140.53.6
01/24/22-02:25:08.907834	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64549	8.8.8.8	192.168.2.4
01/24/22-02:25:08.993738	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	4141	192.168.2.4	185.140.53.6
01/24/22-02:25:14.871570	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63153	8.8.8.8	192.168.2.4

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/24/22-02:25:14.965823	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	4141	192.168.2.4	185.140.53.6
01/24/22-02:25:21.071315	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	4141	192.168.2.4	185.140.53.6
01/24/22-02:25:27.268831	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49782	4141	192.168.2.4	185.140.53.6
01/24/22-02:25:33.435841	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56534	8.8.8.8	192.168.2.4
01/24/22-02:25:33.543043	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49788	4141	192.168.2.4	185.140.53.6
01/24/22-02:25:39.718199	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49789	4141	192.168.2.4	185.140.53.6
01/24/22-02:25:45.786163	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49791	4141	192.168.2.4	185.140.53.6
01/24/22-02:25:51.826837	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49792	4141	192.168.2.4	185.140.53.6
01/24/22-02:25:58.115693	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49810	4141	192.168.2.4	185.140.53.6
01/24/22-02:26:04.066618	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50601	8.8.8.8	192.168.2.4
01/24/22-02:26:04.236531	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49827	4141	192.168.2.4	185.140.53.6
01/24/22-02:26:10.220319	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60875	8.8.8.8	192.168.2.4
01/24/22-02:26:10.485870	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49831	4141	192.168.2.4	185.140.53.6
01/24/22-02:26:16.639258	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56448	8.8.8.8	192.168.2.4
01/24/22-02:26:16.719867	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49833	4141	192.168.2.4	185.140.53.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 02:24:20.164705038 CET	49735	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:20.700340986 CET	4141	49735	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:20.700464010 CET	49735	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:20.743769884 CET	49735	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:21.016308069 CET	4141	49735	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:21.016460896 CET	49735	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:21.349014997 CET	4141	49735	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:21.349283934 CET	49735	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:21.448935986 CET	4141	49735	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:21.467855930 CET	49735	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:21.753155947 CET	4141	49735	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:21.753386974 CET	49735	4141	192.168.2.4	185.140.53.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 02:24:22.075184107 CET	4141	49735	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:22.075364113 CET	49735	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:22.369034052 CET	4141	49735	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:22.369168997 CET	49735	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:22.544080019 CET	49735	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:22.647011995 CET	4141	49735	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:22.647120953 CET	49735	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:26.625017881 CET	49742	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:26.700880051 CET	4141	49742	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:26.701059103 CET	49742	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:26.701611042 CET	49742	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:26.815442085 CET	4141	49742	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:31.237526894 CET	49743	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:31.332380056 CET	4141	49743	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:31.332499981 CET	49743	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:31.333066940 CET	49743	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:31.577058077 CET	4141	49743	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:31.577172995 CET	49743	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:31.879667997 CET	4141	49743	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:31.879786015 CET	49743	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:32.297938108 CET	49743	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:32.381290913 CET	4141	49743	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:32.886949062 CET	49743	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:32.983927965 CET	4141	49743	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:32.990437984 CET	4141	49743	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:33.045161009 CET	49743	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:33.198896885 CET	49743	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:37.408591032 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:37.492502928 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:37.492675066 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:37.493200064 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:37.705472946 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:37.705645084 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:38.014137030 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:38.014259100 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:38.120289087 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:38.120460987 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:38.442538023 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:38.442656040 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:38.739780903 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:38.739892960 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:38.925431013 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:38.925496101 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:38.925570011 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:38.925636053 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.027493000 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.027575970 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.027606010 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.027632952 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.027653933 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.027689934 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.027729034 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.027741909 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.114506960 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.114573002 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.114648104 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.114703894 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.114970922 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.115108967 CET	49750	4141	192.168.2.4	185.140.53.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 02:24:39.115176916 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.115255117 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.115474939 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.115552902 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.115881920 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.115948915 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.174792051 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.174853086 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.174916983 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.174967051 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.206656933 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.207770109 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.245146990 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.245316029 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.251425982 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.251528025 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.251646042 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.251745939 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.252021074 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.252074957 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.252114058 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.252130032 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.252171040 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.252187014 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.252223969 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.252243996 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.252274990 CET	49750	4141	192.168.2.4	185.140.53.6
Jan 24, 2022 02:24:39.252302885 CET	4141	49750	185.140.53.6	192.168.2.4
Jan 24, 2022 02:24:39.252331018 CET	49750	4141	192.168.2.4	185.140.53.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 02:24:20.130364895 CET	59123	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:24:20.152194977 CET	53	59123	8.8.8.8	192.168.2.4
Jan 24, 2022 02:24:26.604687929 CET	54531	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:24:26.623925924 CET	53	54531	8.8.8.8	192.168.2.4
Jan 24, 2022 02:24:31.216694117 CET	49714	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:24:31.236319065 CET	53	49714	8.8.8.8	192.168.2.4
Jan 24, 2022 02:24:37.260209084 CET	58028	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:24:37.283354044 CET	53	58028	8.8.8.8	192.168.2.4
Jan 24, 2022 02:24:43.306494951 CET	53097	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:24:43.325751066 CET	53	53097	8.8.8.8	192.168.2.4
Jan 24, 2022 02:24:50.347665071 CET	62389	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:24:50.367348909 CET	53	62389	8.8.8.8	192.168.2.4
Jan 24, 2022 02:24:56.356394053 CET	49910	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:24:56.376116037 CET	53	49910	8.8.8.8	192.168.2.4
Jan 24, 2022 02:25:02.409034967 CET	55854	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:25:02.430704117 CET	53	55854	8.8.8.8	192.168.2.4
Jan 24, 2022 02:25:08.887145996 CET	64549	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:25:08.907834053 CET	53	64549	8.8.8.8	192.168.2.4
Jan 24, 2022 02:25:14.852178097 CET	63153	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:25:14.871570110 CET	53	63153	8.8.8.8	192.168.2.4
Jan 24, 2022 02:25:20.936527014 CET	52991	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:25:20.955882072 CET	53	52991	8.8.8.8	192.168.2.4
Jan 24, 2022 02:25:27.008050919 CET	51726	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:25:27.027782917 CET	53	51726	8.8.8.8	192.168.2.4
Jan 24, 2022 02:25:33.414751053 CET	56534	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:25:33.435841084 CET	53	56534	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 02:25:39.569437981 CET	56627	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:25:39.586961031 CET	53	56627	8.8.8.8	192.168.2.4
Jan 24, 2022 02:25:45.674490929 CET	56621	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:25:45.694015980 CET	53	56621	8.8.8.8	192.168.2.4
Jan 24, 2022 02:25:51.681771994 CET	63116	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:25:51.704018116 CET	53	63116	8.8.8.8	192.168.2.4
Jan 24, 2022 02:25:57.978744984 CET	55046	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:25:57.998338938 CET	53	55046	8.8.8.8	192.168.2.4
Jan 24, 2022 02:26:04.045773983 CET	50601	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:26:04.066617966 CET	53	50601	8.8.8.8	192.168.2.4
Jan 24, 2022 02:26:10.198947906 CET	60875	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:26:10.220319033 CET	53	60875	8.8.8.8	192.168.2.4
Jan 24, 2022 02:26:16.618215084 CET	56448	53	192.168.2.4	8.8.8.8
Jan 24, 2022 02:26:16.639257908 CET	53	56448	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 24, 2022 02:24:20.130364895 CET	192.168.2.4	8.8.8.8	0xf62e	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:24:26.604687929 CET	192.168.2.4	8.8.8.8	0xcfe8	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:24:31.216694117 CET	192.168.2.4	8.8.8.8	0xbee8	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:24:37.260209084 CET	192.168.2.4	8.8.8.8	0x8d19	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:24:43.306494951 CET	192.168.2.4	8.8.8.8	0xd83c	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:24:50.347665071 CET	192.168.2.4	8.8.8.8	0x3947	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:24:56.356394053 CET	192.168.2.4	8.8.8.8	0xd465	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:02.409034967 CET	192.168.2.4	8.8.8.8	0x9325	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:08.887145996 CET	192.168.2.4	8.8.8.8	0xc690	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:14.852178097 CET	192.168.2.4	8.8.8.8	0xd813	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:20.936527014 CET	192.168.2.4	8.8.8.8	0xa7ba	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:27.008050919 CET	192.168.2.4	8.8.8.8	0x6dd9	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:33.414751053 CET	192.168.2.4	8.8.8.8	0xd584	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:39.569437981 CET	192.168.2.4	8.8.8.8	0x3bc	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:45.674490929 CET	192.168.2.4	8.8.8.8	0x5c16	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:51.681771994 CET	192.168.2.4	8.8.8.8	0xe7ef	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:57.978744984 CET	192.168.2.4	8.8.8.8	0xf5f7	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:26:04.045773983 CET	192.168.2.4	8.8.8.8	0x588d	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:26:10.198947906 CET	192.168.2.4	8.8.8.8	0x7508	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)
Jan 24, 2022 02:26:16.618215084 CET	192.168.2.4	8.8.8.8	0x1c3a	Standard query (0)	onyeoma.ddns.net	A (IP address)	IN (0x0001)

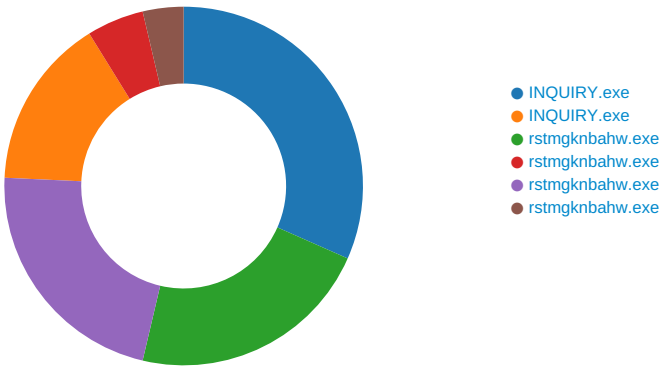
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 24, 2022 02:24:20.152194977 CET	8.8.8.8	192.168.2.4	0xf62e	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:24:26.623925924 CET	8.8.8.8	192.168.2.4	0xcfe8	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 24, 2022 02:24:31.236319065 CET	8.8.8.8	192.168.2.4	0xbee8	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:24:37.283354044 CET	8.8.8.8	192.168.2.4	0x8d19	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:24:43.325751066 CET	8.8.8.8	192.168.2.4	0xd83c	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:24:50.367348909 CET	8.8.8.8	192.168.2.4	0x3947	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:24:56.376116037 CET	8.8.8.8	192.168.2.4	0xd465	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:02.430704117 CET	8.8.8.8	192.168.2.4	0x9325	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:08.907834053 CET	8.8.8.8	192.168.2.4	0xc690	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:14.871570110 CET	8.8.8.8	192.168.2.4	0xd813	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:20.955882072 CET	8.8.8.8	192.168.2.4	0xa7ba	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:27.027782917 CET	8.8.8.8	192.168.2.4	0x6dd9	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:33.435841084 CET	8.8.8.8	192.168.2.4	0xd584	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:39.586961031 CET	8.8.8.8	192.168.2.4	0x3bc	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:45.694015980 CET	8.8.8.8	192.168.2.4	0x5c16	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:51.704018116 CET	8.8.8.8	192.168.2.4	0xe7ef	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:25:57.998338938 CET	8.8.8.8	192.168.2.4	0xf5f7	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:26:04.066617966 CET	8.8.8.8	192.168.2.4	0x588d	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:26:10.220319033 CET	8.8.8.8	192.168.2.4	0x7508	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)
Jan 24, 2022 02:26:16.639257908 CET	8.8.8.8	192.168.2.4	0x1c3a	No error (0)	onyeoma.ddns.net		185.140.53.6	A (IP address)	IN (0x0001)

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: INQUIRY.exe PID: **6904**, Parent PID: **6092**

General

Start time:	02:24:10
Start date:	24/01/2022
Path:	C:\Users\user\Desktop\INQUIRY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\INQUIRY.exe"
Imagebase:	0x400000
File size:	315125 bytes
MD5 hash:	DC0ACC75361BB39FBD4ABEC6EDC82CD5
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: 00000001.00000002.665449354.00000000022E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.665449354.00000000022E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.665449354.00000000022E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.665449354.00000000022E0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	403218	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsc48D4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4057BE	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsc48D5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4057BE	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsc48D6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4057BE	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsc48D6.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\m30xh3rgrf9sf7w0k	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405788	CreateFileA
C:\Users\user\AppData\Local\Temp\taudoswyo	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405788	CreateFileA
C:\Users\user\AppData\Local\Temp\nsc48D6.tmp\gerys.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405788	CreateFileA
C:\Users\user\AppData\Roaming\sspgadrjncoy	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	21A1B88	CreateDirectoryW
C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	21A1D3E	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsc48D4.tmp	success or wait	1	40339E	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsc48D6.tmp	success or wait	1	4053CE	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsc48D5.tmp	0	32768	fd 5c 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 01 00 00 00 fd 05 00 00 46 02 00 00 6c 45 00 00 00 00 00 00 fd 5b 00 00 01 00 00 00 6d 5c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd fd 00 02 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	\,FIE[m\	success or wait	18	403134	WriteFile
C:\Users\user\AppData\Local\Temp\m30xh3rgrf9sf7w0k	0	16384	fd fd 38 fd fd 27 18 05 fd fd bd 01 22 16 38 fd 60 1f 3b 5a fd 74 05 7e fd fd 12 34 fd fd fd 52 0f 5f fd fd 21 5b fd 07 fd 6a 39 42 fd 02 5b 66 1a 45 24 3c 52 26 fd 28 fd 3d fd fd fd 50 fd fd 2a 7b 6d fd fd 2d fd 5d fd 1b 47 1c 23 fd fd 27 fd 04 fd 44 fd 29 fd fd fd 7e 60 10 fd fd 22 fd fd fd 7b 00 30 fd 13 fd 35 55 fd 4c fd 4c fd fd fd 1f 3f 41 fd 70 fd 35 fd 33 74 77 18 fd fd fd 36 fd fd fd 7c 56 57 1c 75 24 09 07 5c fd fd 37 fd fd fd 1c c5 76 02 fd 74 54 4b fd fd 3c 3f fd fd 63 66 15 fd 3a fd 14 2d 17 0f 32 0d fd 67 fd 04 fd 1c fd 01 02 fd fd fd fd fd 11 6a fd 5d fd 41 fd fd fd fd 6e 6e 7e fd fd 4e 65 2d fd 23 3d 27 fd fd 23 fd 0d fd fd fd 13 35 66 47 65 47 fd 85 6b fd 08 fd 36 fd 35 7e 41 fd 33 fd 7c 59 fd 43 2b fd 14 fd 26	8'"8`;Zt~R_![j9B[fE$<R&(=P*{m-]G#'D)~`'" {05ULL? Ap53tw6\|VWu$\7vtTK<? cf:-2gj]An~Ne-#='#5fGeGk65~A3|YC+&	success or wait	17	402FCD	WriteFile
C:\Users\user\AppData\Local\Temp\taudoswyo	0	7539	0b fd 71 74 74 7f fd 08 fd 08 fd fd fd fd fd fd fd 74 49 fd 34 fd 49 45 fd 14 49 fd 34 fd 49 45 fd 0c fd fd fd 74 31 fd fd 4c 74 74 74 fd fd fd 74 39 5f 68 39 5f 44 fd 04 0c fd 74 74 74 fd fd fd 7f fd 39 5f 68 39 5f 44 fd 04 0c 0c 74 74 74 fd 04 fd 7f 00 39 5f 68 39 5f 44 fd 04 0c 05 74 74 74 fd 2c fd 7f 28 39 5f 68 39 5f 44 fd 04 0c fd 74 74 74 fd 34 fd 7f 30 fd 57 44 70 62 1e fd 6c 7c fd 34 75 75 fd 68 fd fd 14 fd 7f 10 fd 44 fd 0c 70 25 2b fd 0c fd 08 fd 0c fd fd fd 70 33 25 06 fd 44 7b fd fd fd 0c 75 7f fd fd 70 36 fd 01 fd fd fd fd 10 fd 25 0c 74 74 74 74 fd 70 50 6f 2d 4d fd fd 39 5f fd 7b 39 5f 04 7e 39 5f 2c fd 7c 39 5f 34 fd 7b 39 5f 14 59 39 5f 0c 7a fd fd 60 44 fd fd fd 68 fd	qtttI4IEI4IEt1Ltttt9_h9_Dttt9_h9_Dttt9_h9_Dttt, (9_h9_Dttt40W Dpbl|4uuhDp%+p3%D{up 6%ttttpPo-M9_{9_~9_,|9_4{9_Y9_z` Dh	success or wait	1	402FCD	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsc48D6.tmp\gerys.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 51 fd fd fd 30 fd fd fd 30 fd fd fd 30 fd fd fd 5b fd fd fd 30 fd fd fd 30 fd fd fd 30 fd fd 4c 6e fd fd fd 30 fd fd 4c 6e fd fd fd 30 fd fd 49 6e 03 fd fd 30 fd fd 4c 6e fd fd fd 30 fd fd 52 69 63 68 fd 30 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd fd 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 00 00 38 00	MZ@!L!This program cannot be run in DOS mode.$Q000[000Ln0Ln0In0Ln0Rich0PELa!8	success or wait	2	402FCD	WriteFile
C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe	0	315125	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 75 4a fd fd 14 24 fd fd 14 24 fd fd 14 24 fd 2f 1c 7b fd fd 14 24 fd fd 14 25 fd 3a 14 24 fd 22 1c 79 fd fd 14 24 fd fd 37 14 fd fd 14 24 fd 66 12 22 fd fd 14 24 fd 52 69 63 68 fd 14 24 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd fd fd 48 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 5a 00 00 00 fd 01 00 00 04 00 00 25 32 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$uJ$$$/{$%:$"y7f"$Rich$PELHZ%2	success or wait	1	21A1D53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\INQUIRY.exe	unknown	512	success or wait	101	4031C5	ReadFile
C:\Users\user\Desktop\INQUIRY.exe	unknown	4	success or wait	1	4031C5	ReadFile
C:\Users\user\Desktop\INQUIRY.exe	unknown	16384	success or wait	17	4031C5	ReadFile
C:\Users\user\AppData\Local\Temp\nsc48D5.tmp	unknown	4	success or wait	1	402F57	ReadFile
C:\Users\user\AppData\Local\Temp\nsc48D5.tmp	unknown	23685	success or wait	1	40300D	ReadFile
C:\Users\user\AppData\Local\Temp\nsc48D5.tmp	unknown	4	success or wait	3	402F57	ReadFile
C:\Users\user\AppData\Local\Temp\nsc48D5.tmp	unknown	16384	success or wait	20	402FB1	ReadFile
C:\Users\user\AppData\Local\Temp\taudoswyo	unknown	7539	success or wait	1	728B1155	ReadFile
C:\Users\user\AppData\Local\Temp\m30xh3rgrf9sf7w0k	unknown	278527	success or wait	1	21A0B37	ReadFile
C:\Users\user\Desktop\INQUIRY.exe	unknown	315125	success or wait	1	21A1D14	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	21A0520	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	21A0520	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	5	21A0520	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	21A0520	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	21A0520	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	earyw	unicode	C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe	success or wait	1	21A1ABB	RegSetValueExW

Analysis Process: INQUIRY.exe PID: **7084**, Parent PID: **6904**

General

Start time:	02:24:12
Start date:	24/01/2022
Path:	C:\Users\user\Desktop\INQUIRY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\INQUIRY.exe"
Imagebase:	0x400000
File size:	315125 bytes
MD5 hash:	DC0ACC75361BB39FBD4ABEC6EDC82CD5
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: 00000002.00000000.662575253.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000000.662575253.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000000.662575253.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.918404744.0000000002522000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.918404744.0000000002522000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.918404744.0000000002522000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.917467270.0000000000774000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.917467270.0000000000774000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.917467270.0000000000774000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.916471993.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.916471993.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.916471993.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.916471993.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000000.663644960.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000000.663644960.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000000.663644960.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.918375056.00000000024E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.918375056.00000000024E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.918375056.00000000024E0000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.918375056.00000000024E0000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.918797240.00000000039A2000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	49E0A09	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	49E0B03	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	49E0A09	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	49E0A09	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	16	49E0B03	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\INQUIRY.exe:Zone.Identifier	success or wait	1	49E0DA9	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	6b 3d 17 3e fd fd fd 48	k=>H	success or wait	1	49E0CBB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 3b fd fd 04 20 53 fd 12 1c fd 7d 46 46 fd 32 fd fd fd 68 fd 4d 2b fd 39 fd fd 4c fd 23 fd 58 fd fd 2b fd fd fd 01 fd fd 2a fd fd 1e fd 7e 66 1e 47 30 5e e9 56 3b fd 2e fd fd 57 32 fd 3d 10 fd fd 4b fd 7e fd 4c 1f 15 26 66 fd fd 2e 70 fd 04 1b fd fd fd 0f fd fd fd 0b 10 3a 37 72 48 7d fd fd fd 0d 2f 48 16 fd fd 06 17 fd 4c fd fd 04 3f fd fd 04 41 08 4b 07 fd fd 4a 17 3d 38 78 21 19 fd fd fd 2b fd 32 65 27 fd 1f 45 3f fd 47 11 fd fd fd 01 fd 5b 00 26	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i S}FF2hM+L#X+*~fG0^;. W2=K~L&f.p:7rH}/HL? AKJ=8x!+2e'E?G[&	success or wait	13	49E0CBB	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	4	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	49E0CBB	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7234BF06	unknown

Analysis Process: rstmgknbahw.exe PID: **6472**, Parent PID: **3424**

General

Start time:	02:24:23
Start date:	24/01/2022
Path:	C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe"
Imagebase:	0x400000
File size:	315125 bytes
MD5 hash:	DC0ACC75361BB39FBD4ABEC6EDC82CD5
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: 00000003.00000002.704939952.0000000002300000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.704939952.0000000002300000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.704939952.0000000002300000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.704939952.0000000002300000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	403218	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsz8149.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4057BE	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsz814A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4057BE	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsz814B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4057BE	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsz814B.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsz814B.tmp\gerys.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405788	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsz8149.tmp	success or wait	1	40339E	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsz814B.tmp	success or wait	1	4053CE	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsz814A.tmp	0	32768	fd 5c 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 01 00 00 00 fd 05 00 00 46 02 00 00 6c 45 00 00 00 00 00 00 fd 5b 00 00 01 00 00 00 6d 5c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd 00 02 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	\,FIE[m\	success or wait	18	403134	WriteFile
C:\Users\user\AppData\Local\Temp\m30xh3rgrf9sf7w0k	0	16384	fd fd 38 fd fd 27 18 05 fd fd bd 01 22 16 38 fd 60 1f 3b 5a fd 74 05 7e fd fd 12 34 fd fd fd 52 0f 5f fd fd 21 5b fd 07 fd 6a 39 42 fd 02 5b 66 1a 45 24 3c 52 26 fd 28 fd 3d fd fd fd 50 fd fd 2a 7b 6d fd fd 2d fd 5d fd 1b 47 1c 23 fd fd 27 fd 04 fd 44 fd 29 fd fd fd 7e 60 10 fd fd 22 fd fd fd 7b 00 30 fd 13 fd 35 55 fd 4c fd 4c fd fd fd 1f 3f 41 fd 70 fd 35 fd 33 74 77 18 fd fd fd 36 fd fd fd 7c 56 57 1c 75 24 09 07 5c fd fd 37 fd fd fd 1c c5 76 02 fd 74 54 4b fd fd 3c 3f fd fd 63 66 15 fd 3a fd 14 2d 17 0f 32 0d fd 67 fd 04 fd 1c fd 01 02 fd fd fd fd fd 11 6a fd 5d fd 41 fd fd fd fd 6e 6e 7e fd fd 4e 65 2d fd 23 3d 27 fd fd 23 fd 0d fd fd fd 13 35 66 47 65 47 fd 85 6b fd 08 fd 36 fd 35 7e 41 fd 33 fd 7c 59 fd 43 2b fd 14 fd 26	8'"8`;Zt~R_![j9B[fE$<R&(=P*{m-]G#'D)~`"{05ULL?Ap53tw6\|VWu$\7vtTK<?cf:-2gj]An~Ne-#='#5fGeGk65~A3|YC+&	success or wait	17	402FCD	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\taudoswyo	0	7539	0b fd 71 74 74 7f fd 08 fd 08 fd fd fd fd fd fd fd 74 49 fd 34 fd 49 45 fd 14 49 fd 34 fd 49 45 fd 0c fd fd fd 74 31 fd fd 4c 74 74 74 fd fd fd 74 39 5f 68 39 5f 44 fd 04 0c fd 74 74 74 fd fd fd 7f fd 39 5f 68 39 5f 44 fd 04 0c 0c 74 74 74 fd 04 fd 7f 00 39 5f 68 39 5f 44 fd 04 0c 05 74 74 74 fd 2c fd 7f 28 39 5f 68 39 5f 44 fd 04 0c fd 74 74 74 fd 34 fd 7f 30 fd 57 44 70 62 1e fd 6c 7c fd 34 75 75 fd 68 fd fd 14 fd 7f 10 fd 44 fd 0c 70 25 2b fd 0c fd 08 fd 0c fd fd fd 70 33 25 06 fd 44 7b fd fd fd 0c 75 7f fd fd 70 36 fd 01 fd fd fd fd 10 fd 25 0c 74 74 74 74 fd 70 50 6f 2d 4d fd fd 39 5f fd 7b 39 5f 04 7e 39 5f 2c fd 7c 39 5f 34 fd 7b 39 5f 14 59 39 5f 0c 7a fd fd 60 44 fd fd fd 68 fd	qtttl4IEI4IEt1Ltttt9_h9_Dtt9_h9_Dttt9_h9_Dttt, (9_h9_Dttt40W Dpbl|4uuhDp%+p3%D{up6%ttttpPo-M9_{9_~9_,|9_4{9_Y9_z`Dh	success or wait	1	402FCD	WriteFile
C:\Users\user\AppData\Local\Temp\nsz814B.tmp\gerys.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 51 fd fd fd 30 fd fd fd 30 fd fd fd 30 fd fd fd 5b fd fd fd 30 fd fd fd 30 fd fd fd 30 fd fd 4c 6e fd fd fd 30 fd fd 4c 6e fd fd fd 30 fd fd 49 6e 03 fd fd 30 fd fd 4c 6e fd fd fd 30 fd fd 52 69 63 68 fd 30 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd fd 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 00 00 38 00	MZ@!L!This program cannot be run in DOS mode.$Q000[000Ln0Ln0In0Ln0Rich0PELa!8	success or wait	2	402FCD	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe	unknown	512	success or wait	101	4031C5	ReadFile
C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe	unknown	4	success or wait	1	4031C5	ReadFile
C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe	unknown	16384	success or wait	17	4031C5	ReadFile
C:\Users\user\AppData\Local\Temp\nsz814A.tmp	unknown	4	success or wait	1	402F57	ReadFile
C:\Users\user\AppData\Local\Temp\nsz814A.tmp	unknown	23685	success or wait	1	40300D	ReadFile
C:\Users\user\AppData\Local\Temp\nsz814A.tmp	unknown	4	success or wait	3	402F57	ReadFile
C:\Users\user\AppData\Local\Temp\nsz814A.tmp	unknown	16384	success or wait	20	402FB1	ReadFile
C:\Users\user\AppData\Local\Temp\taudoswyo	unknown	7539	success or wait	1	6FB01155	ReadFile

Analysis Process: rstmgknbahw.exe PID: **1904**, Parent PID: **6472**

General

Start time:	02:24:29
Start date:	24/01/2022
Path:	C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe"
Imagebase:	0x400000
File size:	315125 bytes
MD5 hash:	DC0ACC75361BB39FBD4ABEC6EDC82CD5
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: 00000004.00000001.703365040.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000001.703365040.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000001.703365040.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000001.703365040.0000000000400000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.723024476.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.723024476.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.723024476.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.723024476.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.725072072.0000000002510000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.725072072.0000000002510000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.725072072.0000000002510000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.725072072.0000000002510000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.725158787.00000000038D1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.725158787.00000000038D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.725158787.00000000038D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.725196610.000000000390A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.725196610.000000000390A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.725133013.00000000028DE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.701936247.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.701936247.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.701936247.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.724570206.00000000006C5000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.724570206.00000000006C5000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.724570206.00000000006C5000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.702725030.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.702725030.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.702725030.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.725281266.00000000049D2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.725281266.00000000049D2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.725281266.00000000049D2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\rstmgknbahw.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	722634A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\rstmgknbahw.exe.log	0	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",03,"	success or wait	1	7254A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile

Analysis Process: rstmgknbahw.exe PID: **4296**, Parent PID: **3424**

General

Start time:	02:24:31
Start date:	24/01/2022
Path:	C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe"
Imagebase:	0x400000
File size:	315125 bytes
MD5 hash:	DC0ACC75361BB39FBD4ABEC6EDC82CD5
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: 00000005.00000002.719731750.0000000002400000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.719731750.0000000002400000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.719731750.0000000002400000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.719731750.0000000002400000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	403218	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsv9D9B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4057BE	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsv9D9C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4057BE	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsv9D9D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4057BE	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsv9D9D.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsv9D9D.tmp\gerys.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405788	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsv9D9B.tmp	success or wait	1	40339E	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsv9D9D.tmp	success or wait	1	4053CE	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsv9D9C.tmp	0	32768	fd 5c 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 01 00 00 00 fd 05 00 00 46 02 00 00 6c 45 00 00 00 00 00 00 fd 5b 00 00 01 00 00 00 6d 5c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd fd 00 02 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	\,FIE[m\	success or wait	18	403134	WriteFile

<table>
<thead>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
</thead>
<tbody>
<tr><td>C:\Users\user\AppData\Local\Temp\m30xh3rgrf9sf7w0k</td><td>0</td><td>16384</td><td>fd fd 38 fd fd 27 18 05 fd fd bd 01 22 16 38 fd 60 1f 3b 5a fd 74 05 7e fd fd 12 34 fd fd fd 52 0f 5f fd fd 21 5b fd 07 fd 6a 39 42 fd 02 5b 66 1a 45 24 3c 52 26 fd 28 fd 3d fd fd fd 50 fd fd 2a 7b 6d fd fd 2d fd 5d fd 1b 47 1c 23 fd fd 27 fd 04 fd 44 fd 29 fd fd fd 7e 60 10 fd fd 22 fd fd fd 7b 00 30 fd 13 fd 35 55 fd 4c fd 4c fd fd fd 1f 3f 41 fd 70 fd 35 fd 33 74 77 18 fd fd fd 36 fd fd fd 7c 56 57 1c 75 24 09 07 5c fd fd 37 fd fd fd 1c c5 76 02 fd 74 54 4b fd fd 3c 3f fd fd 63 66 15 fd 3a fd 14 2d 17 0f 32 0d fd 67 fd 04 fd 1c fd 01 02 fd fd fd fd fd 11 6a fd 5d fd 41 fd fd fd fd 6e 6e 7e fd fd 4e 65 2d fd 23 3d 27 fd fd 23 fd 0d fd fd fd 13 35 66 47 65 47 fd 85 6b fd 08 fd 36 fd 35 7e 41 fd 33 fd 7c 59 fd 43 2b fd 14 fd 26</td><td>8'"8`;Zt~R_![j9B[fE$<R&(=P*{m-]G#'D)~`" {05ULL? Ap53tw6|VWu$\7vtTK<? cf:-2gj]An~Ne- #='#5fGeGk65~A3|YC+&</td><td>success or wait</td><td>17</td><td>402FCD</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\taudoswyo</td><td>0</td><td>7539</td><td>0b fd 71 74 74 7f fd 08 fd 08 fd fd fd fd fd fd fd 74 49 fd 34 fd 49 45 fd 14 49 fd 34 fd 49 45 fd 0c fd fd fd 74 31 fd fd 4c 74 74 74 fd fd fd 74 39 5f 68 39 5f 44 fd 04 0c fd 74 74 74 fd fd fd 7f fd 39 5f 68 39 5f 44 fd 04 0c 0c 74 74 74 fd 04 fd 7f 00 39 5f 68 39 5f 44 fd 04 0c 05 74 74 74 fd 2c fd 7f 28 39 5f 68 39 5f 44 fd 04 0c fd 74 74 74 fd 34 fd 7f 30 fd 57 44 70 62 1e fd 6c 7c fd 34 75 75 fd 68 fd fd 14 fd 7f 10 fd 44 fd 0c 70 25 2b fd 0c fd 08 fd 0c fd fd fd 70 33 25 06 fd 44 7b fd fd fd 0c 75 7f fd fd 70 36 fd 01 fd fd fd fd 10 fd 25 0c 74 74 74 74 fd 70 50 6f 2d 4d fd fd 39 5f fd 7b 39 5f 04 7e 39 5f 2c fd 7c 39 5f 34 fd 7b 39 5f 14 59 39 5f 0c 7a fd fd 60 44 fd fd fd 68 fd</td><td>qtttI4IEI4IEt1Ltttt9_h9_Dttt9_h9_Dttt9_h9_Dttt, (9_h9_Dttt40W Dpbl|4uuhDp%+p3%D{up 6%ttttpPo- M9_{9_~9_,|9_4{9_Y9_z` Dh</td><td>success or wait</td><td>1</td><td>402FCD</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsv9D9D.tmp\gerys.dll</td><td>0</td><td>16384</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 51 fd fd fd 30 fd fd fd 30 fd fd fd 30 fd fd fd 5b fd fd fd 30 fd fd fd 30 fd fd fd 30 fd fd 4c 6e fd fd fd 30 fd fd 4c 6e fd fd fd 30 fd fd 49 6e 03 fd fd 30 fd fd 4c 6e fd fd fd 30 fd fd 52 69 63 68 fd 30 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd fd 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 00 00 38 00</td><td>MZ@!L!This program cannot be run in DOS mode.$Q000[000Ln0Ln0In0Ln0Rich0PELa!8</td><td>success or wait</td><td>2</td><td>402FCD</td><td>WriteFile</td></tr>
</tbody>
</table>

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe	unknown	512	success or wait	101	4031C5	ReadFile
C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe	unknown	4	success or wait	1	4031C5	ReadFile
C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe	unknown	16384	success or wait	17	4031C5	ReadFile
C:\Users\user\AppData\Local\Temp\nsv9D9C.tmp	unknown	4	success or wait	1	402F57	ReadFile
C:\Users\user\AppData\Local\Temp\nsv9D9C.tmp	unknown	23685	success or wait	1	40300D	ReadFile
C:\Users\user\AppData\Local\Temp\nsv9D9C.tmp	unknown	4	success or wait	3	402F57	ReadFile
C:\Users\user\AppData\Local\Temp\nsv9D9C.tmp	unknown	16384	success or wait	20	402FB1	ReadFile
C:\Users\user\AppData\Local\Temp\taudoswyo	unknown	7539	success or wait	1	6F3A1155	ReadFile

Analysis Process: rstmgknbahw.exe PID: **5320**, Parent PID: **4296**

General

Start time:	02:24:37
Start date:	24/01/2022
Path:	C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\sspgadrjncoy\rstmgknbahw.exe"
Imagebase:	0x400000
File size:	315125 bytes
MD5 hash:	DC0ACC75361BB39FBD4ABEC6EDC82CD5
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: 00000006.00000002.735100285.0000000004940000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.735100285.0000000004940000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.735100285.0000000004940000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.735100285.0000000004940000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000000.716081773.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000000.716081773.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000000.716081773.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000001.718977051.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000001.718977051.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000001.718977051.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.734941801.00000000027AE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.735022366.00000000037DA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.735022366.00000000037DA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.734234340.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.734234340.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.734234340.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.734234340.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.735138898.0000000004982000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.735138898.0000000004982000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.735138898.0000000004982000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.734386129.0000000000625000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.734386129.0000000000625000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.734386129.0000000000625000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.734985665.00000000037A1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.734985665.00000000037A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.734985665.00000000037A1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000000.718272419.0000000000414000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000000.718272419.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000000.718272419.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine .config	unknown	4095	success or wait	1	722A8738	ReadFile

Disassembly

No disassembly