ID: 509016
Sample Name: 6811A4CEA56365431B3799600303C945593A997E61968.exe
Cookbook: default.jbs
Time: 22:05:34
Date: 25/10/2021
Version: 33.0.0 White Diamond

Table of Contents

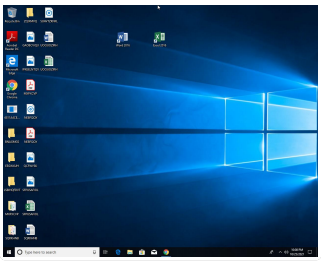
Windows Analysis Report 6811A4CEA56365431B379960…

Overview

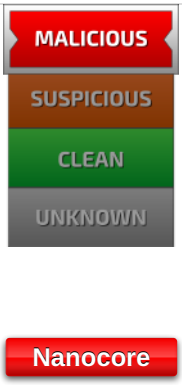
General Information

Sample Name:	6811A4CEA56365431B3799600303C945593A997E61968.exe
Analysis ID:	509016
MD5:	b161113ed44310..
SHA1:	b3a8d24f6b43c44.
SHA256:	6811a4cea56365..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

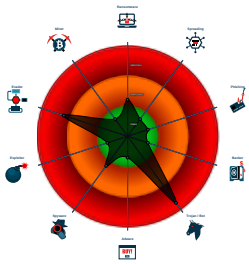


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Machine Learning detection for samp…
- .NET source code contains potentia…
- Machine Learning detection for dropp…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w10x64**
- 6811A4CEA56365431B3799600303C945593A997E61968.exe (PID: 6692 cmdline: 'C:\Users\user\Desktop\6811A4CEA56365431B3799600303C945593A997E61968.exe' MD5: B161113ED44310E65C3D704C0550D668)
- dhcpmon.exe (PID: 7096 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: B161113ED44310E65C3D704C0550D668)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "f211aa87-950c-4609-b635-0852d30e",
  "Group": "Default",
  "Domain1": "softtrim.hopto.org",
  "Domain2": "softtrim.hopto.org",
  "Port": 54984,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "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

Initial Sample

Source	Rule	Description	Author	Strings
6811A4CEA56365431B3799600303C945593A997E61968.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
6811A4CEA56365431B3799600303C945593A997E61968.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
6811A4CEA56365431B3799600303C945593A997E61968.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
6811A4CEA56365431B3799600303C945593A997E61968.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.708062822.000000000375 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000005.00000002.708062822.000000000375 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x23ba3:$a: NanoCore • 0x23bfc:$a: NanoCore • 0x23c39:$a: NanoCore • 0x23cb2:$a: NanoCore • 0x23c05:$b: ClientPlugin • 0x23c42:$b: ClientPlugin • 0x24540:$b: ClientPlugin • 0x2454d:$b: ClientPlugin • 0x1b3fe:$e: KeepAlive • 0x2408d:$g: LogClientMessage • 0x2400d:$i: get_Connected • 0x15bd5:$j: #=q • 0x15c05:$j: #=q • 0x15c41:$j: #=q • 0x15c69:$j: #=q • 0x15c99:$j: #=q • 0x15cc9:$j: #=q • 0x15cf9:$j: #=q • 0x15d29:$j: #=q • 0x15d45:$j: #=q • 0x15d75:$j: #=q
00000005.00000002.708099328.000000000475 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000005.00000002.708099328.000000000475 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x493ad:$a: NanoCore • 0x49406:$a: NanoCore • 0x49443:$a: NanoCore • 0x494bc:$a: NanoCore • 0x5cb67:$a: NanoCore • 0x5cb7c:$a: NanoCore • 0x5cbb1:$a: NanoCore • 0x75633:$a: NanoCore • 0x75648:$a: NanoCore • 0x7567d:$a: NanoCore • 0x4940f:$b: ClientPlugin • 0x4944c:$b: ClientPlugin • 0x49d4a:$b: ClientPlugin • 0x49d57:$b: ClientPlugin • 0x5c923:$b: ClientPlugin • 0x5c93e:$b: ClientPlugin • 0x5c96e:$b: ClientPlugin • 0x5cb85:$b: ClientPlugin • 0x5cbba:$b: ClientPlugin • 0x753ef:$b: ClientPlugin • 0x7540a:$b: ClientPlugin
00000005.00000002.707589854.0000000000FC 2000.00000002.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.dhcpmon.exe.479e404.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
5.2.dhcpmon.exe.479e404.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
5.2.dhcpmon.exe.479e404.3.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
5.2.dhcpmon.exe.3773dc4.1.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
5.2.dhcpmon.exe.3773dc4.1.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 22 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.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)

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

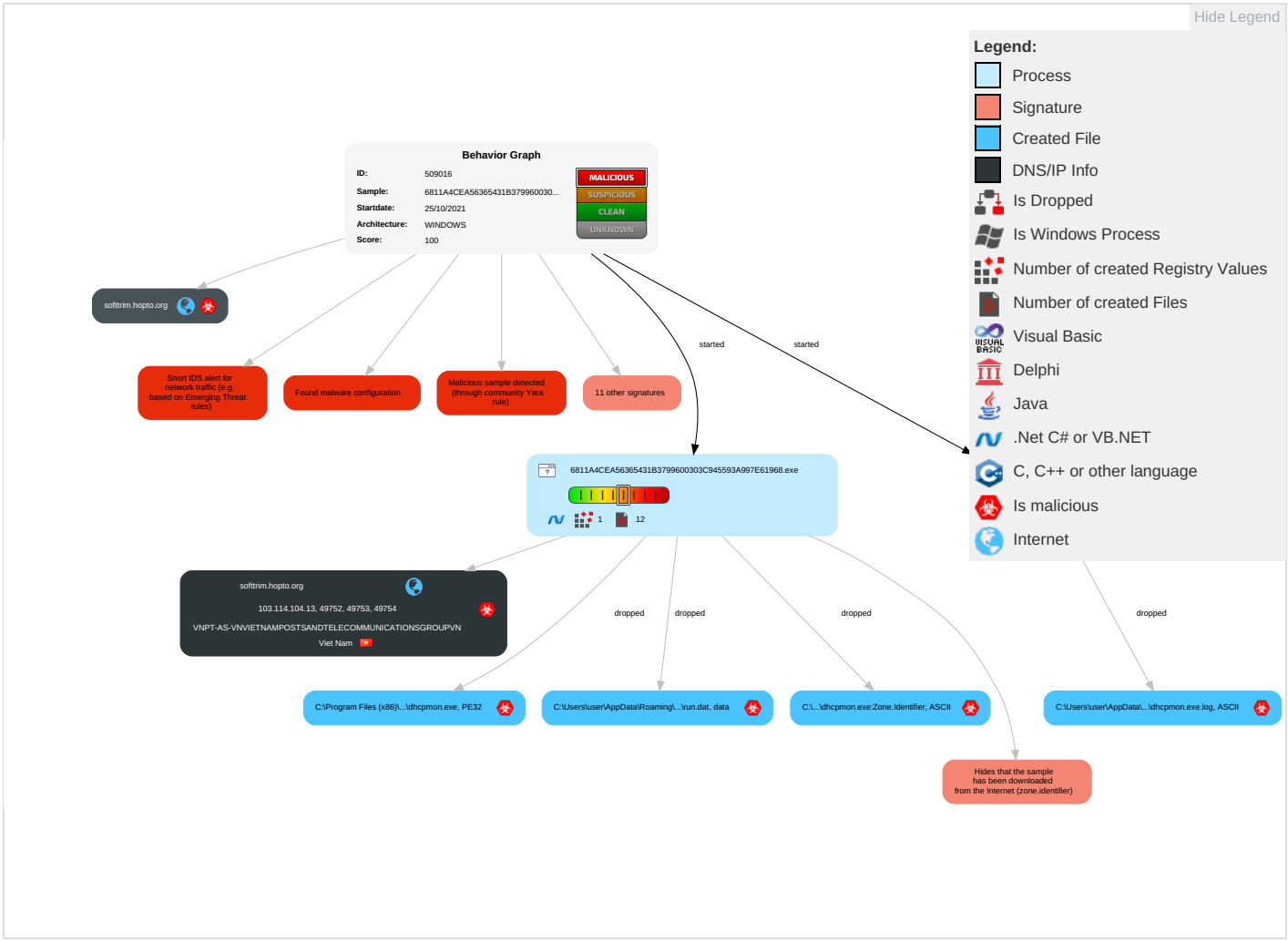
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

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

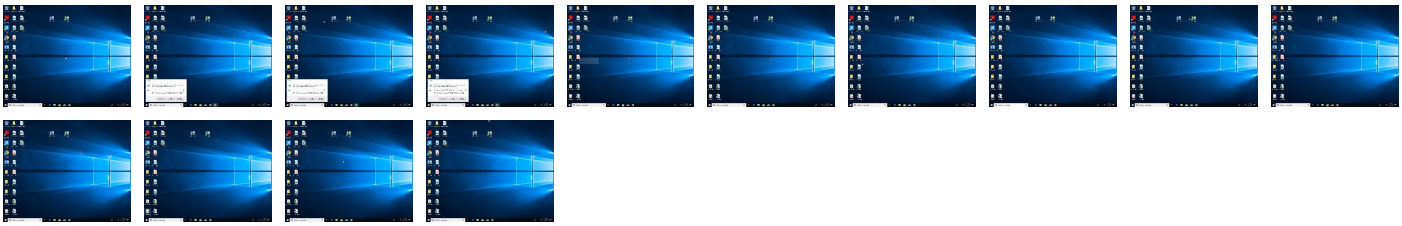
Behavior Graph



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
6811A4CEA56365431B3799600303C945593A997E61968.exe	83%	Virustotal		Browse
6811A4CEA56365431B3799600303C945593A997E61968.exe	86%	Metadefender		Browse
6811A4CEA56365431B3799600303C945593A997E61968.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
6811A4CEA56365431B3799600303C945593A997E61968.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
6811A4CEA56365431B3799600303C945593A997E61968.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	86%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.dhcpmon.exe.fc0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.dhcpmon.exe.fc0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
0.0.6811A4CEA56365431B3799600303C945593A997E61968.exe.cf0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
softtrim.hopto.org	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
softtrim.hopto.org	3%	Virustotal		Browse
softtrim.hopto.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
softtrim.hopto.org	103.114.104.13	true	true	• 3%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
softtrim.hopto.org	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.114.104.13	softtrim.hopto.org	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	509016
Start date:	25.10.2021
Start time:	22:05:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6811A4CEA56365431B3799600303C945593A997E61968.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:	16
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@2/5@21/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
22:06:34	API Interceptor	1046x Sleep call for process: 6811A4CEA56365431B3799600303C945593A997E61968.exe modified
22:06:34	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	KfvEoN0wlw	Get hash	malicious	Browse	• 103.68.250.127
	INQ_42-4I090.xlsx	Get hash	malicious	Browse	• 103.125.190.6
	PO doc 42782.xlsx	Get hash	malicious	Browse	• 103.125.190.6
	b2ZeLApyX2.exe	Get hash	malicious	Browse	• 103.133.109.121
	Purchase order_122.doc	Get hash	malicious	Browse	• 103.133.109.121
	DMS210949 MV LYDERHORN LOW MIX RATIO.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	payment issue need help.exe	Get hash	malicious	Browse	• 103.133.110.241
	DMS210949 MV LYDERHORN LOW MIX RATIO.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	PO1-424480.xlsx	Get hash	malicious	Browse	• 103.125.190.6
	arm7	Get hash	malicious	Browse	• 14.225.246.61
	PI Alu Circle_Dt. 14.05.2021.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	YKr3m9a7C3.exe	Get hash	malicious	Browse	• 103.133.109.121
	SWIFT COPY.doc	Get hash	malicious	Browse	• 103.133.109.121
	Airway bill# 7899865792021.xlsx	Get hash	malicious	Browse	• 103.125.190.6
	presupuesto.xlsx	Get hash	malicious	Browse	• 103.140.251.116

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase orders with bank details.ppa	Get hash	malicious	Browse	• 103.141.138.110
	ZHANGZHOU YIHANSHENG HOUSEWARES.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	PO 4910007391 CHANGZHOU.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	EDG.exe	Get hash	malicious	Browse	• 103.125.189.85
	presupuesto.xlsx	Get hash	malicious	Browse	• 103.140.251.116

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Users\user\Desktop\6811A4CEA56365431B3799600303C945593A997E61968.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207360
Entropy (8bit):	7.44852041350859
Encrypted:	false
SSDEEP:	3072:QzEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIrqskdn+BJCnrylwzt4LLOcsK:QLV6Bta6dtJmakIM5rskxrgztsLPJ
MD5:	B161113ED44310E65C3D704C0550D668
SHA1:	B3A8D24F6B43C44E146DC808EE562C6E1D245C46
SHA-256:	6811A4CEA56365431B3799600303C945593A997E619685D3E98889184CF458C2
SHA-512:	E47D75C508E8E50A393CC4929D36AF9CD58EF62CAB4E64A8E2CC942AF47A61461ACBD3EE28D9DDB4EAFDD3882DFE8AB85A0D07BBF4A696E0EF24F97AD793AC47
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 86%, Browse • Antivirus: ReversingLabs, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. .....8...W.... ...]..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc....]... ...^.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$.....~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\6811A4CEA56365431B3799600303C945593A997E61968.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\6811A4CEA56365431B3799600303C945593A997E61968.exe
File Type:	data
Category:	modified
Size (bytes):	216
Entropy (8bit):	7.012278113302776
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFgwOp7Lr8gVyTwvMV84Miuk:X4LEnybgCF7wHJyCe8Oh
MD5:	0FA1BE38A5A8D2A56F48982C3E9142A6
SHA1:	28E5B087E687E57D4AB6DB352A493AA5657C8484
SHA-256:	4CFA0E50D93A65C81B5CF800F4970E7AD0F7324E0220D1EE91B27D0C0F289493
SHA-512:	F50CA947DCB4F673FADFB6C5F1D9B0FD541679AFD6A03B14719789288A646C4C1762F3E89B8A01B3A87420FDA802B21E5FA109F1FF088898607552172298D83A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S.5.6.C4..E.Y.|.....).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1.....r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL|X

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\6811A4CEA56365431B3799600303C945593A997E61968.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:0y8t:0y8t
MD5:	F98377D310EC6DC16324DCDF628F9628
SHA1:	D3E58FB49FE5E1BE75A8356E1763C36391DED0C4
SHA-256:	44273650DD3C838A88FE11FEB533A8778DBEDEDC6A25CD961274E8E25740189D
SHA-512:	ADB81018AB005FB722DF148415B80A16A761BE8FA538CF4429B05189236A51F28B223A3DB02FB611247CE6459201915BD23C485A3F73202BC83730E65A1B373D
Malicious:	**true**
Reputation:	low
Preview:	......H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.44852041350859

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	6811A4CEA56365431B3799600303C945593A997E61968.exe
File size:	207360
MD5:	b161113ed44310e65c3d704c0550d668
SHA1:	b3a8d24f6b43c44e146dc808ee562c6e1d245c46
SHA256:	6811a4cea56365431b3799600303c945593a997e61968 d3e98889184cf458c2
SHA512:	e47d75c508e8e50a393cc4929d36af9cd58ef62cab4e64a 8e2cc942af47a61461acbd3ee28d9ddb4eafdd3882dfe8a b85a0d07bbf4a696e0ef24f97ad793ac47
SSDEEP:	3072:QzEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIrqskdn+BJCnrylwzt4LLOcsK:QLV6Bta6dtJmakIM5rskxrgztsLPJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41e792
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x54E927A1 [Sun Feb 22 00:49:37 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1c798	0x1c800	False	0.594520970395	data	6.59808518096	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x15d88	0x15e00	False	0.999553571429	data	7.99778830588	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/25/21-22:06:36.007895	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49714	8.8.8.8	192.168.2.4
10/25/21-22:06:36.511244	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	54984	192.168.2.4	103.114.104.13
10/25/21-22:06:42.509658	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58028	8.8.8.8	192.168.2.4
10/25/21-22:06:42.826284	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	54984	192.168.2.4	103.114.104.13
10/25/21-22:06:47.847058	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53097	8.8.8.8	192.168.2.4
10/25/21-22:06:48.143374	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	54984	192.168.2.4	103.114.104.13
10/25/21-22:06:55.592076	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	54984	192.168.2.4	103.114.104.13
10/25/21-22:07:00.374123	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62389	8.8.8.8	192.168.2.4
10/25/21-22:07:00.676570	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	54984	192.168.2.4	103.114.104.13
10/25/21-22:07:07.144852	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55854	8.8.8.8	192.168.2.4
10/25/21-22:07:07.649118	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	54984	192.168.2.4	103.114.104.13
10/25/21-22:07:14.098647	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49760	54984	192.168.2.4	103.114.104.13
10/25/21-22:07:19.187429	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	54984	192.168.2.4	103.114.104.13
10/25/21-22:07:26.936182	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	54984	192.168.2.4	103.114.104.13
10/25/21-22:07:33.666216	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49790	54984	192.168.2.4	103.114.104.13
10/25/21-22:07:39.129307	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49802	54984	192.168.2.4	103.114.104.13
10/25/21-22:07:45.244092	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49612	8.8.8.8	192.168.2.4
10/25/21-22:07:45.548411	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49809	54984	192.168.2.4	103.114.104.13
10/25/21-22:07:52.177600	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49811	54984	192.168.2.4	103.114.104.13
10/25/21-22:07:57.887573	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49834	54984	192.168.2.4	103.114.104.13
10/25/21-22:08:04.610691	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60875	8.8.8.8	192.168.2.4
10/25/21-22:08:04.907955	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49837	54984	192.168.2.4	103.114.104.13
10/25/21-22:08:11.562943	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49838	54984	192.168.2.4	103.114.104.13
10/25/21-22:08:18.116716	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62420	8.8.8.8	192.168.2.4
10/25/21-22:08:18.527714	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49840	54984	192.168.2.4	103.114.104.13
10/25/21-22:08:23.443831	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60579	8.8.8.8	192.168.2.4
10/25/21-22:08:23.762006	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49841	54984	192.168.2.4	103.114.104.13
10/25/21-22:08:28.710325	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49842	54984	192.168.2.4	103.114.104.13
10/25/21-22:08:34.917022	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49843	54984	192.168.2.4	103.114.104.13
10/25/21-22:08:39.747411	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49844	54984	192.168.2.4	103.114.104.13

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 25, 2021 22:06:35.987584114 CEST	192.168.2.4	8.8.8.8	0xa334	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:06:42.489492893 CEST	192.168.2.4	8.8.8.8	0x2d6d	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:06:47.826697111 CEST	192.168.2.4	8.8.8.8	0xa9f3	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:06:55.279752970 CEST	192.168.2.4	8.8.8.8	0xfc29	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:00.353631973 CEST	192.168.2.4	8.8.8.8	0xd831	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:07.123862028 CEST	192.168.2.4	8.8.8.8	0x8f51	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:13.780889988 CEST	192.168.2.4	8.8.8.8	0x101f	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:18.852138996 CEST	192.168.2.4	8.8.8.8	0x194	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:26.623488903 CEST	192.168.2.4	8.8.8.8	0x574b	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:33.347064972 CEST	192.168.2.4	8.8.8.8	0xc73a	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:38.776997089 CEST	192.168.2.4	8.8.8.8	0xd89d	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:45.222021103 CEST	192.168.2.4	8.8.8.8	0xec6b	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:51.861092091 CEST	192.168.2.4	8.8.8.8	0x8d6e	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:57.557805061 CEST	192.168.2.4	8.8.8.8	0x51f9	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:08:04.590718031 CEST	192.168.2.4	8.8.8.8	0x9ca2	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:08:11.214294910 CEST	192.168.2.4	8.8.8.8	0x1080	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:08:18.096024036 CEST	192.168.2.4	8.8.8.8	0xee42	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:08:23.425092936 CEST	192.168.2.4	8.8.8.8	0x9b5d	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:08:28.372742891 CEST	192.168.2.4	8.8.8.8	0x9238	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:08:34.610171080 CEST	192.168.2.4	8.8.8.8	0x6c77	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)
Oct 25, 2021 22:08:39.435587883 CEST	192.168.2.4	8.8.8.8	0x325a	Standard query (0)	softtrim.hopto.org	A (IP address)	IN (0x0001)

DNS Answers

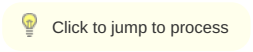
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 22:06:36.007894993 CEST	8.8.8.8	192.168.2.4	0xa334	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:06:42.509658098 CEST	8.8.8.8	192.168.2.4	0x2d6d	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:06:47.847058058 CEST	8.8.8.8	192.168.2.4	0xa9f3	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:06:55.298108101 CEST	8.8.8.8	192.168.2.4	0xfc29	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:00.374123096 CEST	8.8.8.8	192.168.2.4	0xd831	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 22:07:07.144851923 CEST	8.8.8.8	192.168.2.4	0x8f51	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:13.799364090 CEST	8.8.8.8	192.168.2.4	0x101f	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:18.870820045 CEST	8.8.8.8	192.168.2.4	0x194	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:26.642057896 CEST	8.8.8.8	192.168.2.4	0x574b	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:33.365216017 CEST	8.8.8.8	192.168.2.4	0xc73a	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:38.795952082 CEST	8.8.8.8	192.168.2.4	0xd89d	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:45.244091988 CEST	8.8.8.8	192.168.2.4	0xec6b	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:51.879596949 CEST	8.8.8.8	192.168.2.4	0x8d6e	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:07:57.576284885 CEST	8.8.8.8	192.168.2.4	0x51f9	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:08:04.610691071 CEST	8.8.8.8	192.168.2.4	0x9ca2	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:08:11.231417894 CEST	8.8.8.8	192.168.2.4	0x1080	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:08:18.116715908 CEST	8.8.8.8	192.168.2.4	0xee42	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:08:23.443830967 CEST	8.8.8.8	192.168.2.4	0x9b5d	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:08:28.391436100 CEST	8.8.8.8	192.168.2.4	0x9238	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:08:34.628686905 CEST	8.8.8.8	192.168.2.4	0x6c77	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)
Oct 25, 2021 22:08:39.454092026 CEST	8.8.8.8	192.168.2.4	0x325a	No error (0)	softtrim.hopto.org		103.114.104.13	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: 6811A4CEA56365431B3799600303C945593A997E61968.exe PID: 6692 Parent PID: 5348

General

Start time:	22:06:32
Start date:	25/10/2021
Path:	C:\Users\user\Desktop\6811A4CEA56365431B3799600303C945593A997E61968.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\6811A4CEA56365431B3799600303C945593A997E61968.exe'
Imagebase:	0xcf0000
File size:	207360 bytes
MD5 hash:	B161113ED44310E65C3D704C0550D668
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000000.668632002.0000000000CF2000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.668632002.0000000000CF2000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.668632002.0000000000CF2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: dhcpmon.exe PID: 7096 Parent PID: 3424

General

Start time:	22:06:43
Start date:	25/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xfc0000
File size:	207360 bytes
MD5 hash:	B161113ED44310E65C3D704C0550D668
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.708062822.0000000003751000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.708062822.0000000003751000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.708099328.0000000004751000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.708099328.0000000004751000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.707589854.0000000000FC2000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.707589854.0000000000FC2000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.707589854.0000000000FC2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.691691509.0000000000FC2000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.691691509.0000000000FC2000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.691691509.0000000000FC2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 86%, Metadefender, Browse • Detection: 100%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis