ID: 451851
Sample Name:
Contact00212399490.exe
Cookbook: default.jbs
Time: 12:37:11
Date: 21/07/2021
Version: 33.0.0 White Diamond

Table of Contents

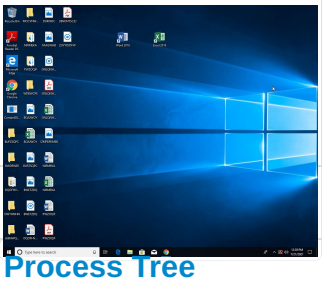
Windows Analysis Report Contact00212399490.exe

Overview

General Information

Sample Name:	Contact00212399490.exe
Analysis ID:	451851
MD5:	fb87d692632732c.
SHA1:	f636d1dba447fd4..
SHA256:	a5a3b625c48719..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

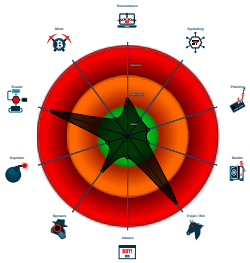
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- Contact00212399490.exe (PID: 6856 cmdline: 'C:\Users\user\Desktop\Contact00212399490.exe' MD5: FB87D692632732CE29ECC8C5AE64F5CF)
  - Contact00212399490.exe (PID: 6852 cmdline: {path} MD5: FB87D692632732CE29ECC8C5AE64F5CF)
    - schtasks.exe (PID: 6564 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp293F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6612 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6492 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp2D28.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Contact00212399490.exe (PID: 6712 cmdline: C:\Users\user\Desktop\Contact00212399490.exe 0 MD5: FB87D692632732CE29ECC8C5AE64F5CF)
  - Contact00212399490.exe (PID: 6032 cmdline: {path} MD5: FB87D692632732CE29ECC8C5AE64F5CF)
- dhcpmon.exe (PID: 7024 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: FB87D692632732CE29ECC8C5AE64F5CF)
  - dhcpmon.exe (PID: 6564 cmdline: {path} MD5: FB87D692632732CE29ECC8C5AE64F5CF)
- dhcpmon.exe (PID: 5908 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: FB87D692632732CE29ECC8C5AE64F5CF)
  - dhcpmon.exe (PID: 5304 cmdline: {path} MD5: FB87D692632732CE29ECC8C5AE64F5CF)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "238a496b-ffb2-448a-bc1f-f27aa516",
  "Group": "Default",
  "Domain1": "",
  "Domain2": "hncbeyghfsbvcuabgsbncvzgaioiuyegdbhabbbw.ydns.eu",
  "Port": 2017,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "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": "8.8.4.415",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000019.00000002.841910692.0000000002EC1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000019.00000002.841910692.0000000002EC1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x238a7:$a: NanoCore • 0x23900:$a: NanoCore • 0x2393d:$a: NanoCore • 0x239b6:$a: NanoCore • 0x23909:$b: ClientPlugin • 0x23946:$b: ClientPlugin • 0x24244:$b: ClientPlugin • 0x24251:$b: ClientPlugin • 0x1b62f:$e: KeepAlive • 0x23d91:$g: LogClientMessage • 0x23d11:$i: get_Connected • 0x158d9:$j: #=q • 0x15909:$j: #=q • 0x15945:$j: #=q • 0x1596d:$j: #=q • 0x1599d:$j: #=q • 0x159cd:$j: #=q • 0x159fd:$j: #=q • 0x15a2d:$j: #=q • 0x15a49:$j: #=q • 0x15a79:$j: #=q
00000019.00000002.841940350.0000000003EC1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000019.00000002.841940350.0000000003EC 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x49ab5:$a: NanoCore • 0x49b0e:$a: NanoCore • 0x49b4b:$a: NanoCore • 0x49bc4:$a: NanoCore • 0x5d26f:$a: NanoCore • 0x5d284:$a: NanoCore • 0x5d2b9:$a: NanoCore • 0x7626b:$a: NanoCore • 0x76280:$a: NanoCore • 0x762b5:$a: NanoCore • 0x49b17:$b: ClientPlugin • 0x49b54:$b: ClientPlugin • 0x4a452:$b: ClientPlugin • 0x4a45f:$b: ClientPlugin • 0x5d02b:$b: ClientPlugin • 0x5d046:$b: ClientPlugin • 0x5d076:$b: ClientPlugin • 0x5d28d:$b: ClientPlugin • 0x5d2c2:$b: ClientPlugin • 0x76027:$b: ClientPlugin • 0x76042:$b: ClientPlugin
00000017.00000002.820461412.00000000040D 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 48 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.dhcpmon.exe.4591288.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
18.2.dhcpmon.exe.4591288.1.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
18.2.dhcpmon.exe.4591288.1.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
18.2.dhcpmon.exe.4591288.1.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
23.2.Contact00212399490.exe.411eb0c.6.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 106 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

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)

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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:

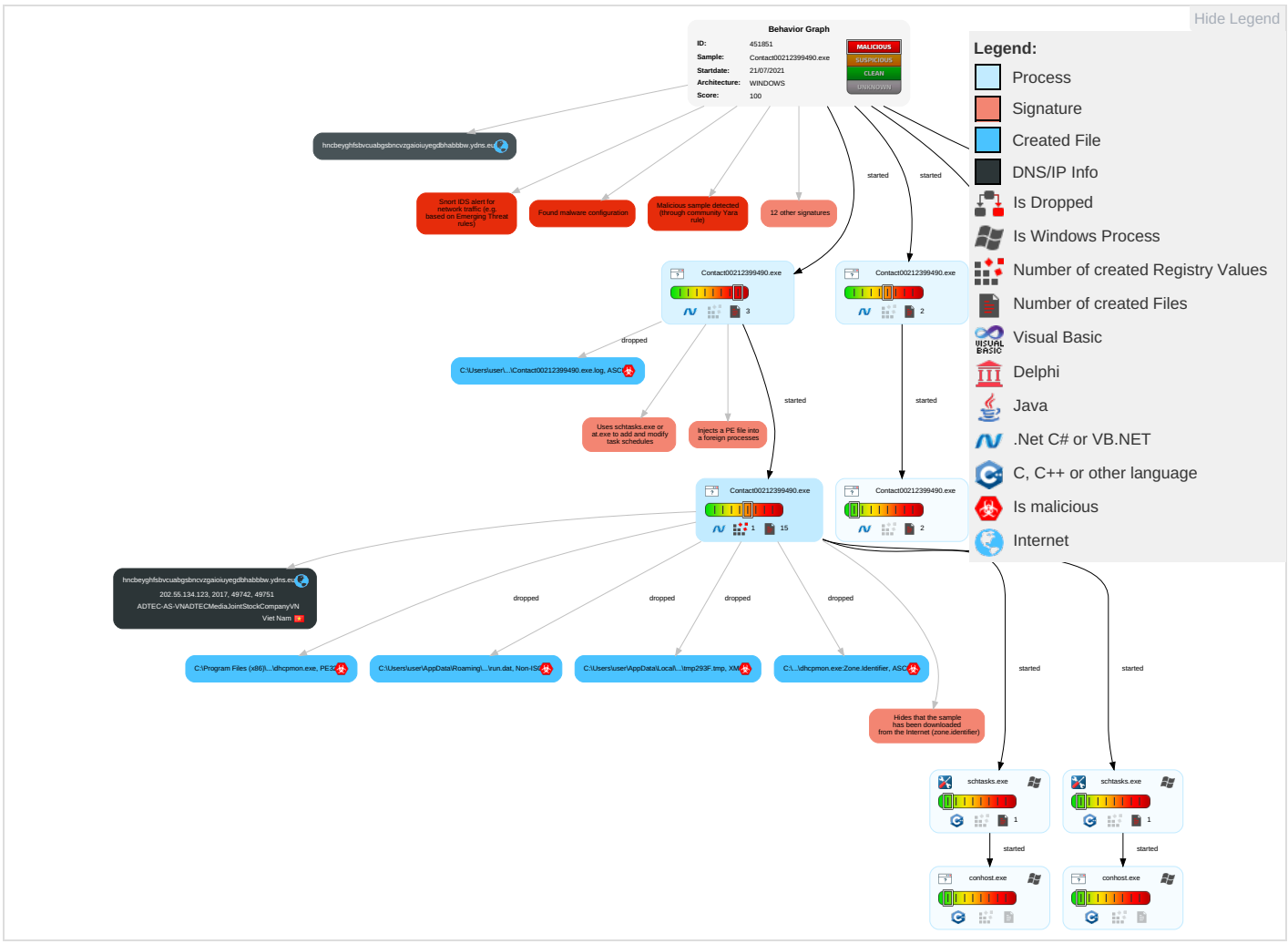
Detected Nanocore Rat

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	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 2	Input Capture 2 1	Security Software Discovery 2 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manip Device Comm
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	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

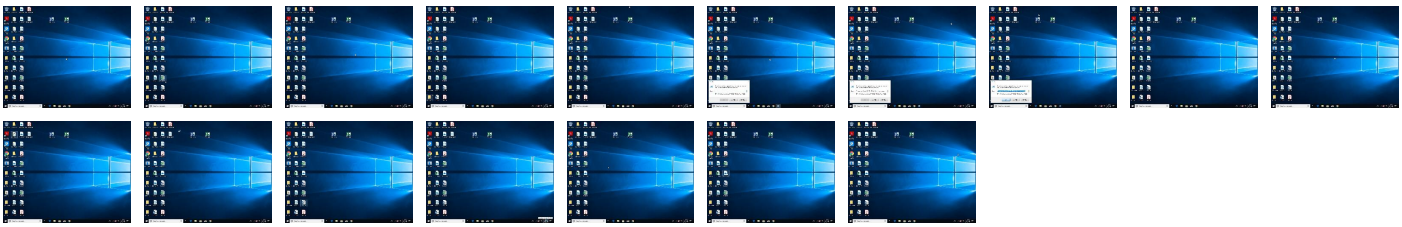
Behavior Graph



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
Contact00212399490.exe	19%	Virustotal		Browse
Contact00212399490.exe	13%	ReversingLabs	ByteCode-MSIL.Trojan.Woreflint	
Contact00212399490.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	13%	ReversingLabs	ByteCode-MSIL.Trojan.Woreflint	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
25.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
23.2.Contact00212399490.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
24.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.Contact00212399490.exe.5c90000.10.unpack	100%	Avira	TR/NanoCore.fadte		Download File
8.2.Contact00212399490.exe.41b7b08.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File
8.2.Contact00212399490.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC_	0%	Avira URL Cloud	safe	
http://www.urwpp.de~=	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.comessed$%	0%	Avira URL Cloud	safe	
http://www.carterandcone.comypo	0%	URL Reputation	safe	
http://www.carterandcone.comypo	0%	URL Reputation	safe	
http://www.carterandcone.comypo	0%	URL Reputation	safe	
http://www.carterandcone.comypo	0%	URL Reputation	safe	
http://www.founder.com.cn/cnp.	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
hncbeyghfsbvcuabgsbncvzgaioiuyegdbhabbbw.ydns.eu	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.founder.com.cn/cnm	0%	URL Reputation	safe	
http://www.founder.com.cn/cnm	0%	URL Reputation	safe	
http://www.founder.com.cn/cnm	0%	URL Reputation	safe	
http://www.fontbureau.comlicd	0%	Avira URL Cloud	safe	
http://www.tiro.comlichG	0%	Avira URL Cloud	safe	
http://www.carterandcone.comypol	0%	Avira URL Cloud	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fonts.comchG	0%	Avira URL Cloud	safe	
http://www.tiro.comFLG9	0%	Avira URL Cloud	safe	
http://www.carterandcone.comuct	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.comic	0%	URL Reputation	safe	
http://www.carterandcone.comic	0%	URL Reputation	safe	
http://www.carterandcone.comic	0%	URL Reputation	safe	
http://www.founder.com.cn/cne	0%	URL Reputation	safe	
http://www.founder.com.cn/cne	0%	URL Reputation	safe	
http://www.founder.com.cn/cne	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/ra	0%	Avira URL Cloud	safe	
http://www.fonts.comn-u	0%	Avira URL Cloud	safe	
http://www.carterandcone.comexcD	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdg$n	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.tiro.comcm?GF	0%	Avira URL Cloud	safe	
http://www.carterandcone.comypoooy	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hncbeyghfsbvcuabgsbncvzgaioiuyegdbhabbbw.ydns.eu	202.55.134.123	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
hncbeyghfsbvcuabgsbncvzgaioiuyegdbhabbbw.ydns.eu	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
202.55.134.123	hncbeyghfsbvcuabgsbncvzgaioiuyegdbhabbbw.ydns.eu	Viet Nam		45540	ADTEC-AS-VNADTECMediaJointStockCompanyVN	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	451851
Start date:	21.07.2021
Start time:	12:37:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Contact00212399490.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:	27
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@18/9@13/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
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
12:38:36	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
12:38:37	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Contact00212399490.exe" s>$(Arg0)
12:38:38	API Interceptor	675x Sleep call for process: Contact00212399490.exe modified
12:38:40	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\Contact00212399490.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	898560
Entropy (8bit):	7.703248488617781
Encrypted:	false
SSDEEP:	24576:mT82zdO4+ysx5W8EtKQaa4Jx4NYDup307r:mY2WyCW8IdadS6o3c
MD5:	FB87D692632732CE29ECC8C5AE64F5CF
SHA1:	F636D1DBA447FD4F579FD4A85A3CC88062759A99
SHA-256:	A5A3B625C48719D4E593435C16795B64D61D25BFEAF20FEAD77C6CAC57241BA4
SHA-512:	8382429513624018B113B5B9470A08DB09399EF4223AC16CC2FB067F0A0B584938420D5591696AE52DD3DCDA945A8B7120BB35038015F0288678E0329C50AFDA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 13%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Kn.`.....0..... .....@.. ..... ..... ..@.....O..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....H....{.....H...XJ.....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.*..*".(.....*..{.... *"..}....*...0..... ....(..... ....(.....(....o.....+R..(.....(.....(.....,.....(....(.....(.....(.....,.....(....(.....(....-.....o.....+...*.....0._.....0.....(.....(.....(....o.....+R..(.....(.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Contact00212399490.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:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Contact00212399490.exe.log	
Process:	C:\Users\user\Desktop\Contact00212399490.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\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:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp293F.tmp	
Process:	C:\Users\user\Desktop\Contact00212399490.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.12418874087686
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0YEbxxtn:cbk4oL600QydbQxIYODOLedq3Yxj
MD5:	18CD46F44E36B957AB997F35FE871E64
SHA1:	9C24D0D7BD98B7B5BD1198544D17F126B00DD646
SHA-256:	57DF8B050EE800C4397F729C6DE44247C983F28CB326844C1F370377FD94E25D
SHA-512:	277F2CB43E919804723AA0CDABBD6FFAB3EF36DFD94E533D0CC2148AE6D0FB9216F4C2EA80B68E020635404D9FEF986D9212D0BAFBC6E52287DE479AB2F8BF85
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp2D28.tmp	
Process:	C:\Users\user\Desktop\Contact00212399490.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704

C:\Users\user\AppData\Local\Temp\tmp2D28.tmp	
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\Contact00212399490.exe
File Type:	data
Category:	modified
Size (bytes):	2552
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw0:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCe
MD5:	881D2F4B245BF6C5FC7A6CA720D59D5E
SHA1:	4BFC165F42F888943ED858A289D0B7368986AA8A
SHA-256:	79655C30BBE54988E098C7759D7614CB980AAAB2FBB60E7F8937CA8F9C95420F
SHA-512:	22E6D650E1DD3730D7B126B80E262788E0FDDFAA2E1C12B599DC85FB3C23D143A6D5F94D048EBE4BA05382BE2E8C85D996BAC3791E1F4F4808771D29ACC2510
Malicious:	false
Reputation:	unknown
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Contact00212399490.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:3B:R
MD5:	E32B02C0E48C9FECE418577AC3AAC519
SHA1:	5576218D2FF37185E95318845A45593D2F4D0FDC
SHA-256:	C24C9CE4DAFDE4A4B010190BA769588700F02F5B795661A330F302D3D824E429
SHA-512:	0E533248574FE69134E3975E8B0A15BDC6D40AB6EC665ABAFC8C9479ECF6E017DEB7A75E065F49CCC119EBE5B4C9605EE56E9284E8906B2190242C90A9F23036
Malicious:	**true**
Reputation:	unknown
Preview:	p..3L.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\Contact00212399490.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	45
Entropy (8bit):	4.322315530038772
Encrypted:	false
SSDEEP:	3:oNt+WfWmKlxEXWcrJ:oNwvmEx+WcrJ
MD5:	7199C8F3347CA649D0EA1CC1FA7B847F
SHA1:	C912A36AC1B5731C346B7942C3F11FCE03831A44
SHA-256:	F4EF6855EC1D73B5ABB65CE2D2D86230052DA4041B885542ED093C5DCAE68A7A

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
SHA-512:	D53FFDE5CCA4A7B7EEA6B45A15E212FEFCC9EE0E49C01A925D14CA05AE16E42FD1BF3EE4CA0FFCEFFB14701396320513702503 93D74CBA01876087252C8894E8
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\Contact00212399490.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.703248488617781
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:	Contact00212399490.exe
File size:	898560
MD5:	fb87d692632732ce29ecc8c5ae64f5cf
SHA1:	f636d1dba447fd4f579fd4a85a3cc88062759a99
SHA256:	a5a3b625c48719d4e593435c16795b64d61d25bfeaf20fead77c6cac57241ba4
SHA512:	8382429513624018b113b5b9470a08db09399ef4223ac16cc2fb067f0a0b584938420d5591696ae52dd3dcda945a8b7120bb35038015f0288678e0329c50afda
SSDEEP:	24576:mT82zdO4+ysx5W8EtKQaa4Jx4NYDup307r:mY2WyCW8IdadS6o3c
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... Kn.`.....0..... ....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4dcaf2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60F76E4B [Wed Jul 21 00:46:03 2021 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	0xdaaf8	0xdac00	False	0.850891741071	data	7.70970971549	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xde000	0x5e4	0x600	False	0.436197916667	data	4.20784097548	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe0000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/21/21-12:38:41.785937	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	2017	192.168.2.4	202.55.134.123
07/21/21-12:38:48.862384	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	2017	192.168.2.4	202.55.134.123
07/21/21-12:38:56.833319	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	2017	192.168.2.4	202.55.134.123
07/21/21-12:39:03.346151	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	2017	192.168.2.4	202.55.134.123
07/21/21-12:39:10.106709	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49763	2017	192.168.2.4	202.55.134.123
07/21/21-12:39:16.805209	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49764	2017	192.168.2.4	202.55.134.123
07/21/21-12:39:23.706214	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49765	2017	192.168.2.4	202.55.134.123
07/21/21-12:39:31.361944	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49767	2017	192.168.2.4	202.55.134.123
07/21/21-12:39:37.826277	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	2017	192.168.2.4	202.55.134.123
07/21/21-12:39:44.438269	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	2017	192.168.2.4	202.55.134.123
07/21/21-12:39:51.162062	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49771	2017	192.168.2.4	202.55.134.123
07/21/21-12:39:57.975899	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49772	2017	192.168.2.4	202.55.134.123
07/21/21-12:40:04.177794	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49773	2017	192.168.2.4	202.55.134.123

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2021 12:38:41.373922110 CEST	192.168.2.4	8.8.8.8	0x768c	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 12:38:48.574074030 CEST	192.168.2.4	8.8.8.8	0x899	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 12:38:56.533895016 CEST	192.168.2.4	8.8.8.8	0xd94d	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:03.043729067 CEST	192.168.2.4	8.8.8.8	0xfd24	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:09.667246103 CEST	192.168.2.4	8.8.8.8	0xd668	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:16.450242996 CEST	192.168.2.4	8.8.8.8	0x1502	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:23.007823944 CEST	192.168.2.4	8.8.8.8	0xe4f2	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:31.074716091 CEST	192.168.2.4	8.8.8.8	0x30f9	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:37.537983894 CEST	192.168.2.4	8.8.8.8	0x8a1f	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:44.116878033 CEST	192.168.2.4	8.8.8.8	0x4c27	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:50.705631971 CEST	192.168.2.4	8.8.8.8	0xf9e8	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:57.617206097 CEST	192.168.2.4	8.8.8.8	0xb4b9	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 12:40:03.888027906 CEST	192.168.2.4	8.8.8.8	0x85f	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2021 12:38:41.414271116 CEST	8.8.8.8	192.168.2.4	0x768c	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 12:38:48.589274883 CEST	8.8.8.8	192.168.2.4	0x899	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2021 12:38:56.562938929 CEST	8.8.8.8	192.168.2.4	0xd94d	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:03.069916010 CEST	8.8.8.8	192.168.2.4	0xfd24	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:09.680434942 CEST	8.8.8.8	192.168.2.4	0xd668	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:16.504811049 CEST	8.8.8.8	192.168.2.4	0x1502	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:23.021382093 CEST	8.8.8.8	192.168.2.4	0xe4f2	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:31.088162899 CEST	8.8.8.8	192.168.2.4	0x30f9	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:37.551628113 CEST	8.8.8.8	192.168.2.4	0x8a1f	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:44.132482052 CEST	8.8.8.8	192.168.2.4	0x4c27	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:50.721638918 CEST	8.8.8.8	192.168.2.4	0xf9e8	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 12:39:57.630556107 CEST	8.8.8.8	192.168.2.4	0xb4b9	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 12:40:03.904207945 CEST	8.8.8.8	192.168.2.4	0x85f	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Contact00212399490.exe PID: 6856 Parent PID: 5964

General

Start time:	12:37:54
Start date:	21/07/2021
Path:	C:\Users\user\Desktop\Contact00212399490.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Contact00212399490.exe'
Imagebase:	0x6b0000
File size:	898560 bytes
MD5 hash:	FB87D692632732CE29ECC8C5AE64F5CF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.729163060.0000000003DA6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.729163060.0000000003DA6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.729163060.0000000003DA6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Contact00212399490.exe PID: 6852 Parent PID: 6856

General

Start time:	12:38:34
Start date:	21/07/2021
Path:	C:\Users\user\Desktop\Contact00212399490.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x900000
File size:	898560 bytes
MD5 hash:	FB87D692632732CE29ECC8C5AE64F5CF
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: 00000008.00000002.911854568.0000000005C90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.911854568.0000000005C90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.911854568.0000000005C90000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.907399609.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.907399609.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.907399609.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.909997625.00000000041AF000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.911502248.00000000059F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.911502248.00000000059F0000.00000004.00000001.sdmp, Author: Florian Roth
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: schtasks.exe PID: 6564 Parent PID: 6852

General

Start time:	12:38:36
Start date:	21/07/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp293F.tmp'
Imagebase:	0x8c0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6612 Parent PID: 6564

General

Start time:	12:38:36
Start date:	21/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6492 Parent PID: 6852

General

Start time:	12:38:37
Start date:	21/07/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp2D28.tmp'
Imagebase:	0x8c0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: Contact00212399490.exe PID: 6712 Parent PID: 968

General

Start time:	12:38:37
Start date:	21/07/2021
Path:	C:\Users\user\Desktop\Contact00212399490.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Contact00212399490.exe 0
Imagebase:	0x5e0000
File size:	898560 bytes
MD5 hash:	FB87D692632732CE29ECC8C5AE64F5CF
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: 0000000C.00000002.808360718.0000000003C96000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.808360718.0000000003C96000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.808360718.0000000003C96000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: conhost.exe PID: 6720 Parent PID: 6492

General

Start time:	12:38:37
Start date:	21/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 7024 Parent PID: 968

General

Start time:	12:38:40
Start date:	21/07/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xec0000
File size:	898560 bytes
MD5 hash:	FB87D692632732CE29ECC8C5AE64F5CF
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: 0000000E.00000002.818841483.00000000046B6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.818841483.00000000046B6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.818841483.00000000046B6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 13%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 5908 Parent PID: 3424

General

Start time:	12:38:44
Start date:	21/07/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xcf0000
File size:	898560 bytes
MD5 hash:	FB87D692632732CE29ECC8C5AE64F5CF
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: 00000012.00000002.833125664.0000000004466000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.833125664.0000000004466000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.833125664.0000000004466000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: Contact00212399490.exe PID: 6032 Parent PID: 6712

General

Start time:	12:39:12
Start date:	21/07/2021
Path:	C:\Users\user\Desktop\Contact00212399490.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x7b0000
File size:	898560 bytes
MD5 hash:	FB87D692632732CE29ECC8C5AE64F5CF
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: 00000017.00000002.820461412.00000000040D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.820461412.00000000040D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000002.817702789.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.817702789.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.817702789.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.820081893.00000000030D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.820081893.00000000030D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 6564 Parent PID: 7024

General

Start time:	12:39:15
Start date:	21/07/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xac0000
File size:	898560 bytes
MD5 hash:	FB87D692632732CE29ECC8C5AE64F5CF
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: 00000018.00000002.831351914.0000000003351000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.831351914.0000000003351000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.829356083.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.829356083.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.829356083.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.831387157.0000000004351000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.831387157.0000000004351000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 5304 Parent PID: 5908

General

Start time:	12:39:19
Start date:	21/07/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x640000
File size:	898560 bytes
MD5 hash:	FB87D692632732CE29ECC8C5AE64F5CF
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: 00000019.00000002.841910692.0000000002EC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.841910692.0000000002EC1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.841940350.0000000003EC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.841940350.0000000003EC1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000019.00000002.840452566.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.840452566.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.840452566.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Disassembly

Code Analysis