ID: 451970
Sample Name:
Contact00212399490.exe
Cookbook: default.jbs
Time: 16:28:53
Date: 21/07/2021
Version: 33.0.0 White Diamond

Table of Contents

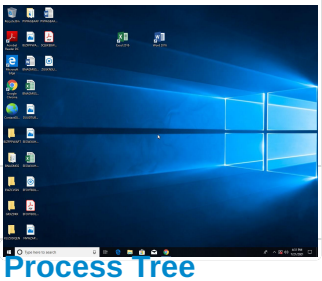
Windows Analysis Report Contact00212399490.exe

Overview

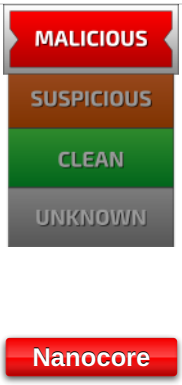
General Information

Sample Name:	Contact00212399490.exe
Analysis ID:	451970
MD5:	a6bd3de048002b..
SHA1:	90cf93d93b14165.
SHA256:	1e3539b9de5113..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

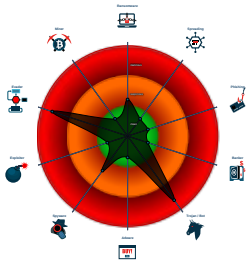


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- 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…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Tries to detect sandboxes and other…
- Uses schtasks.exe or at.exe to add …

Classification



Process Tree

- **System is w10x64**
- Contact00212399490.exe (PID: 5560 cmdline: 'C:\Users\user\Desktop\Contact00212399490.exe' MD5: A6BD3DE048002BEE7A8D973C887227D8)
  - Contact00212399490.exe (PID: 6288 cmdline: {path} MD5: A6BD3DE048002BEE7A8D973C887227D8)
  - Contact00212399490.exe (PID: 6296 cmdline: {path} MD5: A6BD3DE048002BEE7A8D973C887227D8)
    - schtasks.exe (PID: 6332 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp203E.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6340 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6384 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp23F8.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6396 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Contact00212399490.exe (PID: 6424 cmdline: C:\Users\user\Desktop\Contact00212399490.exe 0 MD5: A6BD3DE048002BEE7A8D973C887227D8)
  - Contact00212399490.exe (PID: 5276 cmdline: {path} MD5: A6BD3DE048002BEE7A8D973C887227D8)
- dhcpmon.exe (PID: 6584 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: A6BD3DE048002BEE7A8D973C887227D8)
  - dhcpmon.exe (PID: 6360 cmdline: {path} MD5: A6BD3DE048002BEE7A8D973C887227D8)
- dhcpmon.exe (PID: 6760 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: A6BD3DE048002BEE7A8D973C887227D8)
  - dhcpmon.exe (PID: 6460 cmdline: {path} MD5: A6BD3DE048002BEE7A8D973C887227D8)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.493564138.000000000446 8000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000021.00000002.422634506.000000000370 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000021.00000002.422634506.000000000370 1000.00000004.00000001.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:$j: #=q
00000020.00000002.403561087.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000020.00000002.403561087.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 45 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.Contact00212399490.exe.5f20000.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
18.2.Contact00212399490.exe.5f20000.8.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
18.2.Contact00212399490.exe.5f20000.8.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
23.2.Contact00212399490.exe.3ee6d10.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8J YUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
23.2.Contact00212399490.exe.3ee6d10.1.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
Click to see the 87 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:

Yara detected Nanocore RAT

Networking:

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

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:

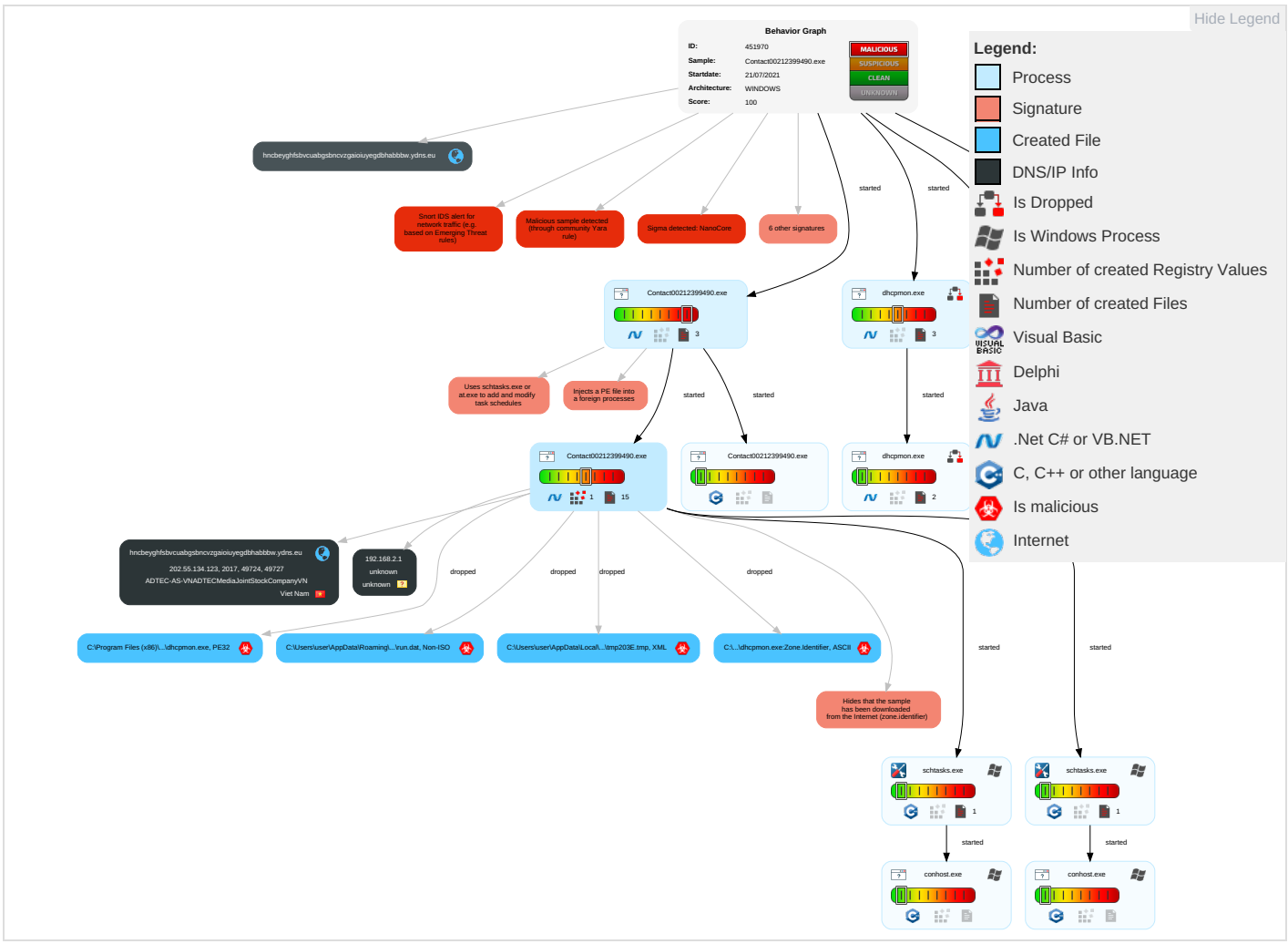
Detected Nanocore Rat

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	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 2	Input Capture 2 1	Security Software Discovery 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	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	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	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)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	System Information Discovery 1 3	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 1	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Ce Base Stat

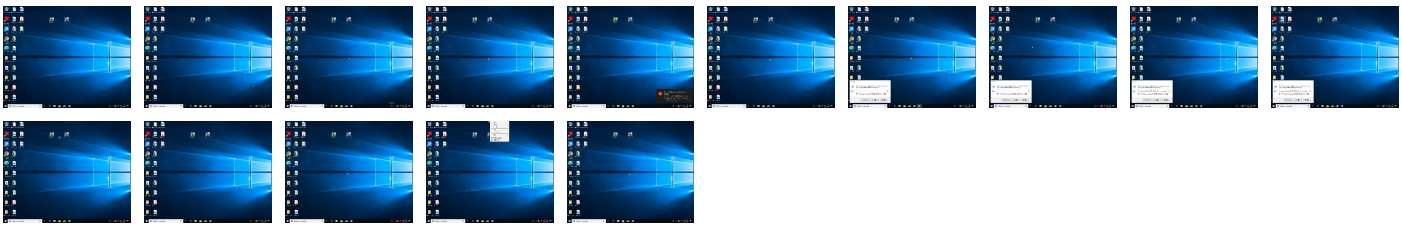
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.Contact00212399490.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
18.2.Contact00212399490.exe.5f20000.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File
18.2.Contact00212399490.exe.4477b08.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File
32.2.Contact00212399490.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
33.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.compor	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnLog	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.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.fonts.comcz	0%	Avira URL Cloud	safe	
http://www.fonts.com-	0%	Avira URL Cloud	safe	
http://www.fonts.comnc	0%	Avira URL Cloud	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.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.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	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.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	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.jiyu-kobo.co.jp/eta	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/yp	0%	Avira URL Cloud	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	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.sandoll.co.krW	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/m	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/m	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/m	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.sandoll.co.krndor	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	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.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.fontbureau.comu	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/f	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/f	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/f	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.tiro.comh	0%	URL Reputation	safe	
http://www.tiro.comh	0%	URL Reputation	safe	
http://www.tiro.comh	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	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.founder.com.cn/cnh	0%	URL Reputation	safe	
http://www.founder.com.cn/cnh	0%	URL Reputation	safe	
http://www.founder.com.cn/cnh	0%	URL Reputation	safe	
http://www.tiro.com$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

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

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	451970
Start date:	21.07.2021

Start time:	16:28:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 46s
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:	38
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@20/9@12/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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
16:30:29	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
16:30:30	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Contact00212399490.exe" s>$(Arg0)
16:30:30	API Interceptor	627x Sleep call for process: Contact00212399490.exe modified
16:30:33	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(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):	1249792
Entropy (8bit):	7.296203531808417
Encrypted:	false
SSDEEP:	24576:UpAJYYuDA0w9KPf5iodHl5Rus+xr9Yipb:UtA59ExiodHjczZ
MD5:	A6BD3DE048002BEE7A8D973C887227D8
SHA1:	90CF93D93B141654A62FF3A3B6810FAEF2FF3D69
SHA-256:	1E3539B9DE51134004FF4BFF43AB144E748A329265DECF8421442CEF3109210D
SHA-512:	6B84954F6DBE9C7D5A7580C2D917414A7875494508A3D17B4F092D270FECBE695E10F6EB27DE52AAC807D06A432E3902DC9A9671C7BC2B170B46AFBA1B6F30 6
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....!.`.....0..*.....NH... ..`....@.. ....@.....G..O....`..$.....`..... ....H.....text...t(... ...*..... ..`.rsrc...$....`.....,.....@..@.rel oc.....`.....@..B.....0H.....H.....P..(.....^.}.....(.....(....*&..(....*...0..+.....,.{.....+....,...{....o.....(....*..0..R.....s.. ..}.....s....}.....s....}.....s....}.....{....o.....(.....{.....s....o.....{.....s....o .....{....r...po!.....{.... ....s"...o#.....{.....o$.....{.....o%.....{.....o&.....{.....o'.....{....r...p"...A.. ....s(...o).....{.... =. ...+s....o.....{.....s....o .....{....r)..po!.....{....

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:	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_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\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\tmp203E.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):	5.127828672196681
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Bbxxtn:cbk4oL600QydbQxIYODOLedq3uxj
MD5:	FF1EAD8DD1A327803CC0AF366C4779BE
SHA1:	5D8B3A64E735C55AD2D37F07E5324A0D07D3759F
SHA-256:	8A7A84F8AA98258FDE30287A469E05946729DC733298243F8E30AA35767A3467
SHA-512:	249FC4E9676141BF6B1922CDD5103AE6F224B0255E15FACB806B190BCE83E8766E7567218C16D537FA469F27CC39D0B98518771B997AEA77CEAFC8CC947BB62
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\tmp23F8.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
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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Size (bytes):	2088
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0llC0llC0llC0llC0llC0llC0llCe
MD5:	0D6805D12813A857D50D42D6EE2CCAB0
SHA1:	78D83F009D842F21FE2AB0EAFFD00E5AAD1776F4
SHA-256:	182E0F8AA959549D61C66D049645BA8445D86AEAD2B8C3552A9836FA1E5BD484
SHA-512:	5B29496F3AB3CCB915CF37042F4956BB00E577B5F15457A5A739BE1BD50C481FB7E3297EED575DCA7A7BD30ECBC140DD3666CD7DEDD25DFB7AEB41A1B5BEI A4A
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 NEL line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Ts/t:yt
MD5:	A8C6CE27FDAD82203BB2ED4E9A023677
SHA1:	A4962AE7B7A6A7435C1EA5452EF02339C9831AA9
SHA-256:	E93547D3CF9BAA27E30936696631627B1BF44F07E2AC6793A0A66AE7E264081E
SHA-512:	8BD3060CCC25656213053CCA1AC1A6EE7EFF8DF3BC9AE9A084A6ACD4EB673D95D3B7B097992C4725DBB1BAA0EA4BD82DE331712203CAFBFBB8C1155CEFCF 6A2B
Malicious:	**true**
Reputation:	unknown
Preview:	/-...L.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):	4.491418651692922
Encrypted:	false
SSDEEP:	3:oNWXp5vmKlxEXWcrJ:oNWXpFmEx+WcrJ
MD5:	4979705993AF30ED02989EE5ACDC91C6
SHA1:	E528A9C66F0045827240596C66B9F1B141503DB1
SHA-256:	3918BA8BED55D1B40797E60A055BE2C5B70069A04D1E8162D510FEA3FA121AFF
SHA-512:	3165B9EF14162D8AAEBF34C8583A2B9094839DC2F5565D6BBCE7F714C78C4B26C9482B55C23BD2B4515D5CD0754FF88BE701A3540958D9D2218826013CFB315
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):	7.296203531808417

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:	Contact00212399490.exe
File size:	1249792
MD5:	a6bd3de048002bee7a8d973c887227d8
SHA1:	90cf93d93b141654a62ff3a3b6810faef2ff3d69
SHA256:	1e3539b9de51134004ff4bff43ab144e748a329265decf8421442cef3109210d
SHA512:	6b84954f6dbe9c7d5a7580c2d917414a7875494508a3d17b4f092d270fecbe695e10f6eb27de52aac807d06a432e3902dc9a9671c7bc2b170b46afba1b6f30c6
SSDEEP:	24576:UpAJYYuDA0w9KPf5iodHl5Rus+xr9Yipb:UtA59ExiodHjczZ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....!.`.....0..*.....NH... ...`....@.. .....@.....

File Icon

Icon Hash:	f0debeffdffeec70

Static PE Info

General

Entrypoint:	0x4d484e
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:	0x60F821D2 [Wed Jul 21 13:32:02 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	0xd2874	0xd2a00	False	0.862556797107	data	7.74858352039	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd6000	0x5e324	0x5e400	False	0.167370378813	data	5.64060790935	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x136000	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
07/21/21-16:30:35.553871	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	2017	192.168.2.3	202.55.134.123
07/21/21-16:30:42.799204	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	2017	192.168.2.3	202.55.134.123
07/21/21-16:30:49.455492	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	2017	192.168.2.3	202.55.134.123
07/21/21-16:30:56.688728	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	2017	192.168.2.3	202.55.134.123
07/21/21-16:31:03.513825	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	2017	192.168.2.3	202.55.134.123
07/21/21-16:31:10.011751	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	2017	192.168.2.3	202.55.134.123
07/21/21-16:31:21.029571	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	2017	192.168.2.3	202.55.134.123
07/21/21-16:31:27.895143	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49749	2017	192.168.2.3	202.55.134.123
07/21/21-16:31:40.457114	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	2017	192.168.2.3	202.55.134.123
07/21/21-16:31:47.386740	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	2017	192.168.2.3	202.55.134.123
07/21/21-16:31:53.546692	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	2017	192.168.2.3	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
Jul 21, 2021 16:30:34.393743992 CEST	192.168.2.3	8.8.8.8	0x5e56	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 16:30:42.493211985 CEST	192.168.2.3	8.8.8.8	0x5844	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 16:30:49.123671055 CEST	192.168.2.3	8.8.8.8	0xff1c	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 16:30:56.191770077 CEST	192.168.2.3	8.8.8.8	0x1a01	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 16:31:03.229469061 CEST	192.168.2.3	8.8.8.8	0xc52b	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2021 16:31:09.695439100 CEST	192.168.2.3	8.8.8.8	0x6ddd	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 16:31:17.659133911 CEST	192.168.2.3	8.8.8.8	0xb620	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 16:31:27.549313068 CEST	192.168.2.3	8.8.8.8	0xec40	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 16:31:34.319772005 CEST	192.168.2.3	8.8.8.8	0x4a6a	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 16:31:40.173595905 CEST	192.168.2.3	8.8.8.8	0x18f3	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 16:31:47.102724075 CEST	192.168.2.3	8.8.8.8	0x8c6a	Standard query (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu	A (IP address)	IN (0x0001)
Jul 21, 2021 16:31:53.261570930 CEST	192.168.2.3	8.8.8.8	0x43f1	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 16:30:34.434061050 CEST	8.8.8.8	192.168.2.3	0x5e56	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 16:30:42.518599033 CEST	8.8.8.8	192.168.2.3	0x5844	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 16:30:49.139580011 CEST	8.8.8.8	192.168.2.3	0xff1c	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 16:30:56.204567909 CEST	8.8.8.8	192.168.2.3	0x1a01	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 16:31:03.242533922 CEST	8.8.8.8	192.168.2.3	0xc52b	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 16:31:09.735086918 CEST	8.8.8.8	192.168.2.3	0x6ddd	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 16:31:17.672297001 CEST	8.8.8.8	192.168.2.3	0xb620	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 16:31:27.589896917 CEST	8.8.8.8	192.168.2.3	0xec40	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 16:31:34.372350931 CEST	8.8.8.8	192.168.2.3	0x4a6a	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 16:31:40.186373949 CEST	8.8.8.8	192.168.2.3	0x18f3	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 16:31:47.115642071 CEST	8.8.8.8	192.168.2.3	0x8c6a	No error (0)	hncbeyghfs bvcuabgsbn cvzgaioiuy egdbhabbbw .ydns.eu		202.55.134.123	A (IP address)	IN (0x0001)
Jul 21, 2021 16:31:53.276655912 CEST	8.8.8.8	192.168.2.3	0x43f1	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: 5560 Parent PID: 5616

General

Start time:	16:29:45
Start date:	21/07/2021
Path:	C:\Users\user\Desktop\Contact00212399490.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Contact00212399490.exe'
Imagebase:	0xe80000
File size:	1249792 bytes
MD5 hash:	A6BD3DE048002BEE7A8D973C887227D8
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: 00000001.00000002.307046969.00000000047D6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.307046969.00000000047D6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.307046969.00000000047D6000.00000004.00000001.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: 6288 Parent PID: 5560

General

Start time:	16:30:25
Start date:	21/07/2021
Path:	C:\Users\user\Desktop\Contact00212399490.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x2e0000
File size:	1249792 bytes
MD5 hash:	A6BD3DE048002BEE7A8D973C887227D8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Contact00212399490.exe PID: 6296 Parent PID: 5560

General

Start time:	16:30:26
Start date:	21/07/2021
Path:	C:\Users\user\Desktop\Contact00212399490.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xb50000
File size:	1249792 bytes
MD5 hash:	A6BD3DE048002BEE7A8D973C887227D8
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: 00000012.00000002.493564138.0000000004468000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.494730709.0000000005F20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.494730709.0000000005F20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.494730709.0000000005F20000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.481278156.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.481278156.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.481278156.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.494575561.0000000005C90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.494575561.0000000005C90000.00000004.00000001.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: 6332 Parent PID: 6296

General

Start time:	16:30:28
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\tmp203E.tmp'
Imagebase:	0xfc0000
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: 6340 Parent PID: 6332

General

Start time:	16:30:28
Start date:	21/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 6384 Parent PID: 6296

General

Start time:	16:30:29
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\tmp23F8.tmp'
Imagebase:	0xfc0000
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: 6396 Parent PID: 6384

General

Start time:	16:30:30
Start date:	21/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: Contact00212399490.exe PID: 6424 Parent PID: 528

General

Start time:	16:30:30
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:	0x4e0000
File size:	1249792 bytes
MD5 hash:	A6BD3DE048002BEE7A8D973C887227D8
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: 00000017.00000002.391430185.0000000003DA6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.391430185.0000000003DA6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.391430185.0000000003DA6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 6584 Parent PID: 528

General

Start time:	16:30:33
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:	0x1f0000
File size:	1249792 bytes
MD5 hash:	A6BD3DE048002BEE7A8D973C887227D8
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: 00000018.00000002.411512020.0000000003966000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.411512020.0000000003966000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.411512020.0000000003966000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 6760 Parent PID: 3388

General

Start time:	16:30:38
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:	0xe0000
File size:	1249792 bytes
MD5 hash:	A6BD3DE048002BEE7A8D973C887227D8
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: 00000019.00000002.413945103.0000000003A36000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.413945103.0000000003A36000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.413945103.0000000003A36000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: Contact00212399490.exe PID: 5276 Parent PID: 6424

General

Start time:	16:31:06
Start date:	21/07/2021
Path:	C:\Users\user\Desktop\Contact00212399490.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x4f0000
File size:	1249792 bytes
MD5 hash:	A6BD3DE048002BEE7A8D973C887227D8
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: 00000020.00000002.403561087.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.403561087.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.403561087.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.409908287.0000000002CF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.409908287.0000000002CF1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.409994109.0000000003CF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.409994109.0000000003CF1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 6360 Parent PID: 6584

General

Start time:	16:31:11
Start date:	21/07/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xdf0000
File size:	1249792 bytes
MD5 hash:	A6BD3DE048002BEE7A8D973C887227D8
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: 00000021.00000002.422634506.0000000003701000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000002.422634506.0000000003701000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000021.00000002.417010887.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000002.417010887.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000002.417010887.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000002.422686382.0000000004701000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000002.422686382.0000000004701000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis