ID: 458708
Sample Name:
vHLZ6AHJFY.exe
Cookbook: default.jbs
Time: 17:05:42
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

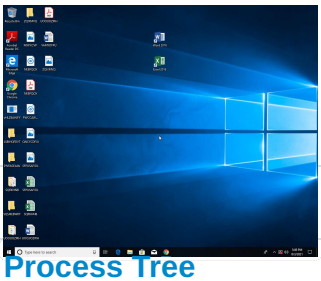
Windows Analysis Report vHLZ6AHJFY.exe

Overview

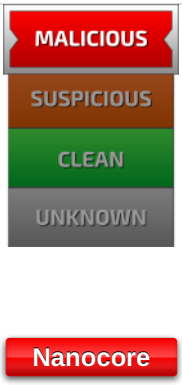
General Information

Sample Name:	vHLZ6AHJFY.exe
Analysis ID:	458708
MD5:	e7f52d9d50e6d27.
SHA1:	3382b97a082773..
SHA256:	fcf8936d333a76b..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



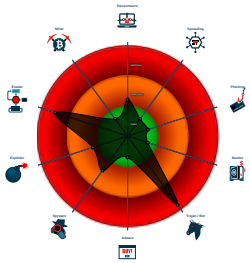
Nanocore

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
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Machine Learning detection for dropp…

Classification



Process Tree

- **System is w10x64**
- vHLZ6AHJFY.exe (PID: 4640 cmdline: 'C:\Users\user\Desktop\vHLZ6AHJFY.exe' MD5: E7F52D9D50E6D2776D301B5A7E03B662)
  - vHLZ6AHJFY.exe (PID: 4832 cmdline: C:\Users\user\Desktop\vHLZ6AHJFY.exe MD5: E7F52D9D50E6D2776D301B5A7E03B662)
- dhcpmon.exe (PID: 2680 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: E7F52D9D50E6D2776D301B5A7E03B662)
  - dhcpmon.exe (PID: 5008 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: E7F52D9D50E6D2776D301B5A7E03B662)
  - dhcpmon.exe (PID: 6008 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: E7F52D9D50E6D2776D301B5A7E03B662)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "6a1c2465-7ac5-4f1d-acc5-ef04fcf4",
  "Group": "Default",
  "Domain1": "hhjhtggfr.duckdns.org",
  "Domain2": "dertrefg.duckdns.org",
  "Port": 8234,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "hhjhtggfr.duckdns.org"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.316057670.0000000002F2 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000D.00000002.316057670.0000000002F2 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x6943f:$a: NanoCore • 0x69498:$a: NanoCore • 0x694d5:$a: NanoCore • 0x6954e:$a: NanoCore • 0x694a1:$b: ClientPlugin • 0x694de:$b: ClientPlugin • 0x69ddc:$b: ClientPlugin • 0x69de9:$b: ClientPlugin • 0x5f0a3:$e: KeepAlive • 0x69929:$g: LogClientMessage • 0x698a9:$i: get_Connected • 0x59875:$j: #=q • 0x598a5:$j: #=q • 0x598e1:$j: #=q • 0x59909:$j: #=q • 0x59939:$j: #=q • 0x59969:$j: #=q • 0x59999:$j: #=q • 0x599c9:$j: #=q • 0x599e5:$j: #=q • 0x59a15:$j: #=q
0000000D.00000002.315036949.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000D.00000002.315036949.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000D.00000002.315036949.000000000040 2000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.dhcpmon.exe.2f89660.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
13.2.dhcpmon.exe.2f89660.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
13.2.dhcpmon.exe.3f74565.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x23c70:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x23c9d:$x2: IClientNetworkHost
13.2.dhcpmon.exe.3f74565.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0x23c70:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0x24d4b:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost • 0x23c8a:$s5: IClientLoggingHost
13.2.dhcpmon.exe.3f74565.3.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 28 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:

- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- .NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Stealing of Sensitive Information:

- Yara detected Nanocore RAT

Remote Access Functionality:

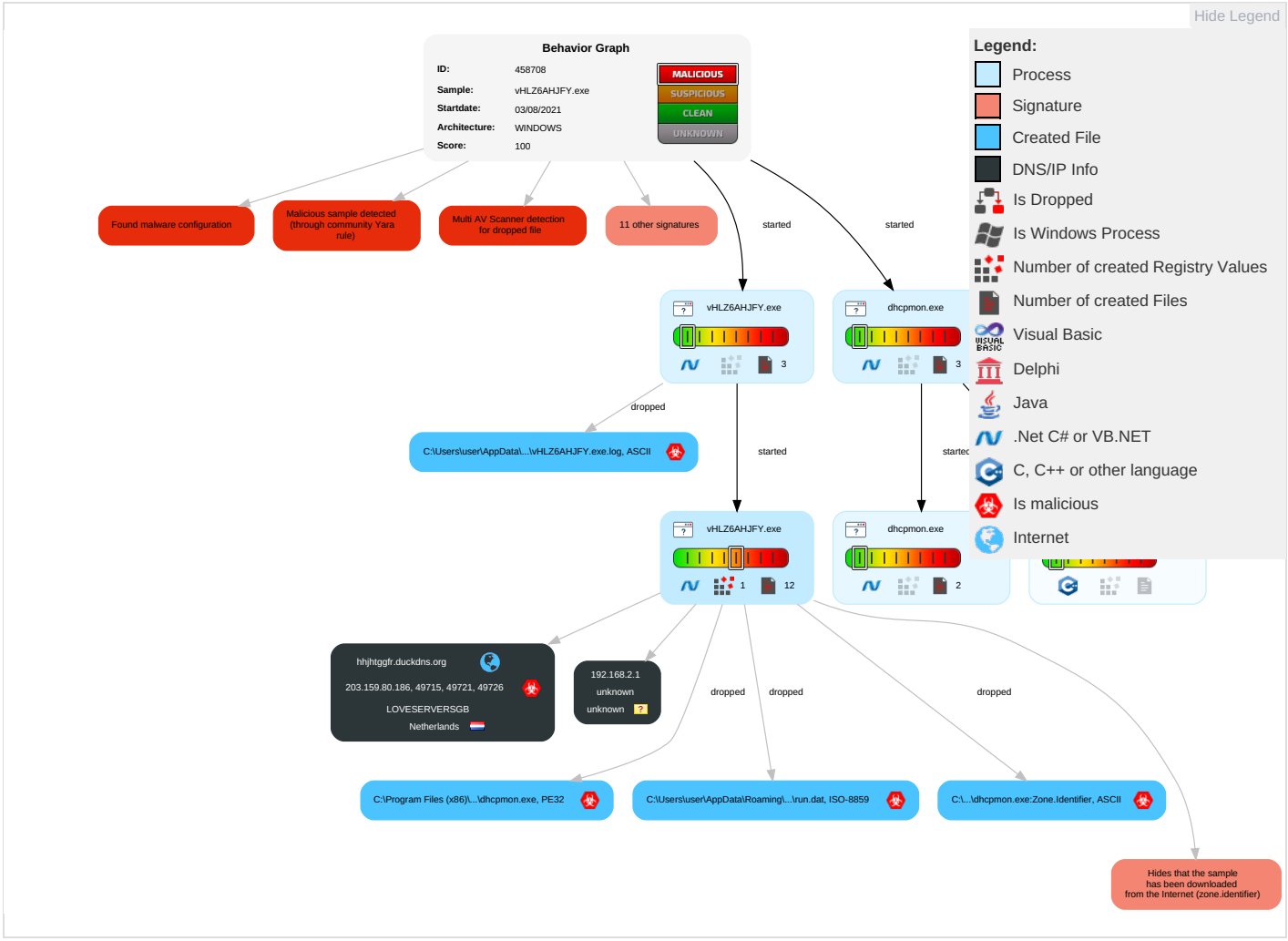
- Detected Nanocore Rat
- Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Eff
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 1	Masquerading 2	Input Capture 2 1	Query Registry 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Ea Ins Ne Co

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Eff
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Ex Re Ca
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Ex Tra Lo
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SI Sw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Ma De Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jar De Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Ro Ac
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	Do Ins Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Ro Ba

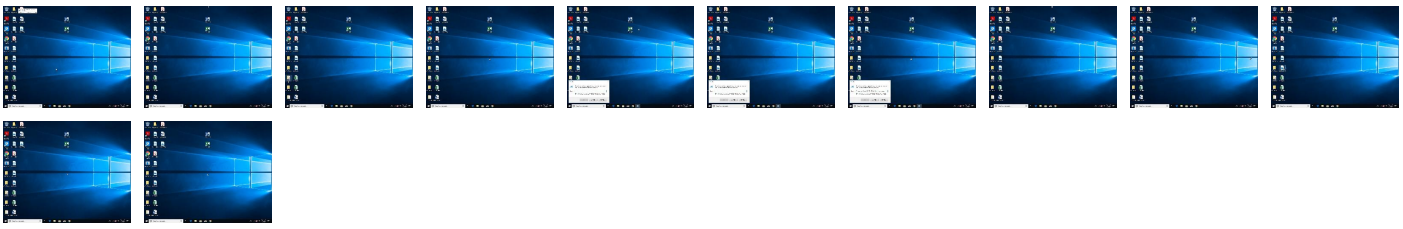
Behavior Graph



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
vHLZ6AHJFY.exe	31%	Virustotal		Browse
vHLZ6AHJFY.exe	22%	ReversingLabs	Win32.Trojan.Pwsx	
vHLZ6AHJFY.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	22%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
hhjhtggfr.duckdns.org	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
dertrefg.duckdns.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hhjhtggfr.duckdns.org	203.159.80.186	true	true		unknown

Contacted URLs

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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.159.80.186	hhjhtggfr.duckdns.org	Netherlands		47987	LOVESERVERSGB	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458708
Start date:	03.08.2021
Start time:	17:05:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 51s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	vHLZ6AHJFY.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@8/8@19/2
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
17:06:36	API Interceptor	1012x Sleep call for process: vHLZ6AHJFY.exe modified
17:06:44	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
17:06:57	API Interceptor	1x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
203.159.80.186	NEW PO1100372954 -.doc	Get hash	malicious	Browse	• newhosteeeee.ydns.eu/putty.exe
	2711164142.doc	Get hash	malicious	Browse	• newhosteeeee.ydns.eu/microF.exe
	N40-MR .doc	Get hash	malicious	Browse	• newhosteeeee.ydns.eu/microC.exe
	N40-MR 311.doc	Get hash	malicious	Browse	• newhosteeeee.ydns.eu/microA.exe
	PO2100382954 -.doc	Get hash	malicious	Browse	• newhosteeeee.ydns.eu/microD.exe
	2fja1Oszs9.exe	Get hash	malicious	Browse	• hutyrtit.ydns.eu/microC.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
hhjhtggfr.duckdns.org	NEW PO1100372954 -.doc	Get hash	malicious	Browse	• 203.159.80.186
	N40-MR 311.doc	Get hash	malicious	Browse	• 203.159.80.186
	Xjf4yH9N2t.exe	Get hash	malicious	Browse	• 203.159.80.186
	wm4J5m8pIK.exe	Get hash	malicious	Browse	• 203.159.80.186
	WrNhr6yUD8.exe	Get hash	malicious	Browse	• 37.0.8.214
	YjnGfifJ4X.exe	Get hash	malicious	Browse	• 203.159.80.101
	E8NURjuahU.exe	Get hash	malicious	Browse	• 203.159.80.101
	MkASxmQle3.exe	Get hash	malicious	Browse	• 203.159.80.101
	6rkqQM8Ldz.exe	Get hash	malicious	Browse	• 203.159.80.101
	bHSfr2q0yu.exe	Get hash	malicious	Browse	• 203.159.80.101
	lqtN3Z5Uzp.exe	Get hash	malicious	Browse	• 203.159.80.101
	Invoice 406496.doc	Get hash	malicious	Browse	• 203.159.80.101
	1OLlrVAlAE.exe	Get hash	malicious	Browse	• 203.159.80.101
	microC.exe	Get hash	malicious	Browse	• 203.159.80.101

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LOVESERVERSGB	Shipping Details.exe	Get hash	malicious	Browse	• 203.159.80.118
	NEW PO1100372954 -.doc	Get hash	malicious	Browse	• 203.159.80.165
	2711164142.doc	Get hash	malicious	Browse	• 203.159.80.165
	N40-MR .doc	Get hash	malicious	Browse	• 203.159.80.186
	N40-MR 311.doc	Get hash	malicious	Browse	• 203.159.80.165
	PO2100382954 -.doc	Get hash	malicious	Browse	• 203.159.80.186
	Xjf4yH9N2t.exe	Get hash	malicious	Browse	• 203.159.80.165
	wm4J5m8pIK.exe	Get hash	malicious	Browse	• 203.159.80.186
	2fja1Oszs9.exe	Get hash	malicious	Browse	• 203.159.80.186
	SKM-582649274924.exe	Get hash	malicious	Browse	• 203.159.80.93
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 203.159.80.118
	eInvoicing.jar	Get hash	malicious	Browse	• 203.159.80.23
	DyxL4y2hv3.exe	Get hash	malicious	Browse	• 203.159.80.165
	ktWmI8zMGs.exe	Get hash	malicious	Browse	• 203.159.80.182
	fBR05jzjti.exe	Get hash	malicious	Browse	• 203.159.80.165
	Original Shipping .doc	Get hash	malicious	Browse	• 203.159.80.165
	hfJdO3BjO0.exe	Get hash	malicious	Browse	• 203.159.80.107
	No.IV21002542.doc	Get hash	malicious	Browse	• 203.159.80.107
	payment details.doc	Get hash	malicious	Browse	• 203.159.80.107
	DblVVdaNgC.exe	Get hash	malicious	Browse	• 203.159.80.107

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\vHLZ6AHJFY.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	835072
Entropy (8bit):	7.439063931141525
Encrypted:	false
SSDEEP:	12288:SZdWFS44N+vWrz4C89yIkjPeO6gSxW61AannR6VJj134bGlvpmjz2iN:SbWFSn+vW4F5yPeJgqWkAYngHj1dpY1
MD5:	E7F52D9D50E6D2776D301B5A7E03B662
SHA1:	3382B97A08277306637E074F08814B728BC225CC
SHA-256:	FCF8936D333A76B64672AE8C445531EFC277C0AD3222720E1C4B43573B681375

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
SHA-512:	924B09B696ED70EF112DE29B61F90AB01E818F901EBA58F21685E95EBE1B4F0810DFBB2D28CDF41B1E1C58CB179EB6DF0A19969180E67ED335EC084E65423FD0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 22%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P..... .....@.. ....@.....O.....x..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....I..... ...X.....0.....(....(.....(.....o.....*.....(.....(!.....("....(#.....($....*N..(....o^...(%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0..<.....~.....(1.....,r..p.....(2...o3...s4.....~.....+..*.0.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\vHLZ6AHJFY.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_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):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vHLZ6AHJFY.exe.log	
Process:	C:\Users\user\Desktop\vHLZ6AHJFY.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vHLZ6AHJFY.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\vHLZ6AHJFY.exe
File Type:	data
Category:	dropped
Size (bytes):	2088
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCe
MD5:	0D6805D12813A857D50D42D6EE2CCAB0
SHA1:	78D83F009D842F21FE2AB0EAFFD00E5AAD1776F4
SHA-256:	182E0F8AA959549D61C66D049645BA8445D86AEAD2B8C3552A9836FA1E5BD484
SHA-512:	5B29496F3AB3CCB915CF37042F4956BB00E577B5F15457A5A739BE1BD50C481FB7E3297EED575DCA7A7BD30ECBC140DD3666CD7DEDD25DFB7AEB41A1B5BEA4A
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\vHLZ6AHJFY.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:N4n:W
MD5:	C2BD38A6DB63769773CAFA759E408A99
SHA1:	C865D09925B221950EEA216FEAEF74C6F9BB4EE9
SHA-256:	D62FD7B51C8B8FBD978A82CE646961CA86E5DEE11C3DA8CCF5DF4877A14E56C6
SHA-512:	627141212397F00ED3D8E24BDAA2E3B1A3C60ADC3779BA24DF96773F87B04D23E98B1393E684C2B90A529C6012E5D87F818408BDDCAB2E07D0D3D24EA02EBFA
Malicious:	**true**
Reputation:	unknown
Preview:	"%:..V.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\vHLZ6AHJFY.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\vHLZ6AHJFY.exe

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Reputation:	unknown
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v."".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.Ql..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.439063931141525
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	vHLZ6AHJFY.exe
File size:	835072
MD5:	e7f52d9d50e6d2776d301b5a7e03b662
SHA1:	3382b97a08277306637e074f08814b728bc225cc
SHA256:	fcf8936d333a76b64672ae8c445531efc277c0ad3222720e1c4b43573b681375
SHA512:	924b09b696ed70ef112de29b61f90ab01e818f901eba58f21685e95ebe1b4f0810dfbb2d28cdf41b1e1c58cb179eb6df0a19969180e67ed335ec084e65423fd0
SSDEEP:	12288:SZdWFS44N+vWrz4C89ylkjPeO6gSxW61AannR6VJj134bGlvpmjz2iN:SbWFSn+vW4F5yPeJgqWkAYngHj1dpY1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... .....P..... .....@.. .... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4cd3e6
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

General

Time Stamp:	0xFAEB95B0 [Sun May 27 21:08:00 2103 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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	0xcb3ec	0xcb400	False	0.789118955643	data	7.44654724316	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xce000	0x5ec	0x600	False	0.430989583333	data	4.2010150696	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd0000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 17:06:41.265094995 CEST	192.168.2.7	8.8.8.8	0xcfe7	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:06:48.393317938 CEST	192.168.2.7	8.8.8.8	0x7cdd	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:06:54.889625072 CEST	192.168.2.7	8.8.8.8	0x11f3	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:00.969794989 CEST	192.168.2.7	8.8.8.8	0x402a	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:07.044657946 CEST	192.168.2.7	8.8.8.8	0xfdca	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:12.698101997 CEST	192.168.2.7	8.8.8.8	0x22a8	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:18.848773003 CEST	192.168.2.7	8.8.8.8	0xe20e	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:24.825263023 CEST	192.168.2.7	8.8.8.8	0xa8bd	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:30.959038019 CEST	192.168.2.7	8.8.8.8	0x6954	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 17:07:37.138364077 CEST	192.168.2.7	8.8.8.8	0xc73b	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:43.207992077 CEST	192.168.2.7	8.8.8.8	0x73b	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:49.125431061 CEST	192.168.2.7	8.8.8.8	0x93cf	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:56.132236004 CEST	192.168.2.7	8.8.8.8	0x9baa	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:08:02.321283102 CEST	192.168.2.7	8.8.8.8	0x992f	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:08:09.583043098 CEST	192.168.2.7	8.8.8.8	0xef63	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:08:16.466579914 CEST	192.168.2.7	8.8.8.8	0xf44b	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:08:22.695369959 CEST	192.168.2.7	8.8.8.8	0xa8b4	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:08:28.805661917 CEST	192.168.2.7	8.8.8.8	0x812	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 17:08:34.787343025 CEST	192.168.2.7	8.8.8.8	0x4c87	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 17:06:41.395359993 CEST	8.8.8.8	192.168.2.7	0xcfe7	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:06:48.524399996 CEST	8.8.8.8	192.168.2.7	0x7cdd	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:06:54.923458099 CEST	8.8.8.8	192.168.2.7	0x11f3	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:01.004370928 CEST	8.8.8.8	192.168.2.7	0x402a	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:07.080137014 CEST	8.8.8.8	192.168.2.7	0xfdca	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:12.732578993 CEST	8.8.8.8	192.168.2.7	0x22a8	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:18.882757902 CEST	8.8.8.8	192.168.2.7	0xe20e	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:24.858367920 CEST	8.8.8.8	192.168.2.7	0xa8bd	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:30.991909981 CEST	8.8.8.8	192.168.2.7	0x6954	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:37.173894882 CEST	8.8.8.8	192.168.2.7	0xc73b	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:43.240693092 CEST	8.8.8.8	192.168.2.7	0x73b	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:49.254106998 CEST	8.8.8.8	192.168.2.7	0x93cf	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:07:56.166098118 CEST	8.8.8.8	192.168.2.7	0x9baa	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:08:02.454139948 CEST	8.8.8.8	192.168.2.7	0x992f	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:08:09.619055033 CEST	8.8.8.8	192.168.2.7	0xef63	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:08:16.499321938 CEST	8.8.8.8	192.168.2.7	0xf44b	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:08:22.728216887 CEST	8.8.8.8	192.168.2.7	0xa8b4	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 17:08:28.840946913 CEST	8.8.8.8	192.168.2.7	0x812	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 3, 2021 17:08:34.821742058 CEST	8.8.8.8	192.168.2.7	0x4c87	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: vHLZ6AHJFY.exe PID: 4640 Parent PID: 5608

General

Start time:	17:06:30
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\vHLZ6AHJFY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\vHLZ6AHJFY.exe'
Imagebase:	0xf0000
File size:	835072 bytes
MD5 hash:	E7F52D9D50E6D2776D301B5A7E03B662
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.243870600.00000000026DB000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.246214384.0000000003559000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.246214384.0000000003559000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.246214384.0000000003559000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: vHLZ6AHJFY.exe PID: 4832 Parent PID: 4640

General

Start time:	17:06:37
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\vHLZ6AHJFY.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\vHLZ6AHJFY.exe
Imagebase:	0x490000
File size:	835072 bytes
MD5 hash:	E7F52D9D50E6D2776D301B5A7E03B662
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: dhcpmon.exe PID: 2680 Parent PID: 3292

General

Start time:	17:06:53
Start date:	03/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x50000
File size:	835072 bytes
MD5 hash:	E7F52D9D50E6D2776D301B5A7E03B662
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000005.00000002.296482527.000000000256B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.302655095.00000000033E9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.302655095.00000000033E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.302655095.00000000033E9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 22%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 5008 Parent PID: 2680

General

Start time:	17:06:59
Start date:	03/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x340000
File size:	835072 bytes
MD5 hash:	E7F52D9D50E6D2776D301B5A7E03B662
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: 6008 Parent PID: 2680

General

Start time:	17:07:00
Start date:	03/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xbc0000
File size:	835072 bytes
MD5 hash:	E7F52D9D50E6D2776D301B5A7E03B662
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: 0000000D.00000002.316057670.0000000002F21000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.316057670.0000000002F21000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.315036949.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.315036949.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.315036949.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.316141333.0000000003F29000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.316141333.0000000003F29000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities — Show Windows behavior

File Created

File Read

Disassembly

Code Analysis