ID: 457788
Sample Name:
wm4J5m8pIK.exe
Cookbook: default.jbs
Time: 10:02:56
Date: 02/08/2021
Version: 33.0.0 White Diamond

Table of Contents

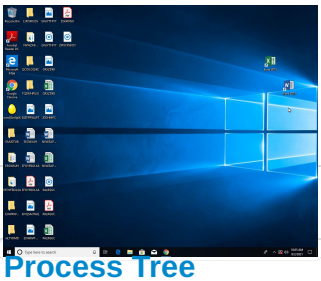
Windows Analysis Report wm4J5m8pIK.exe

Overview

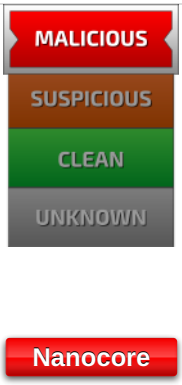
General Information

Sample Name:	wm4J5m8pIK.exe
Analysis ID:	457788
MD5:	8fa8f52dfc55d34…
SHA1:	4fbdb8c39bbc48b..
SHA256:	2c7da7ff43c90ae..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



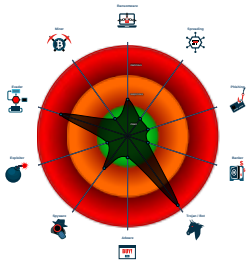
Nanocore

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 doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- .NET source code references suspic…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- wm4J5m8pIK.exe (PID: 5804 cmdline: 'C:\Users\user\Desktop\wm4J5m8pIK.exe' MD5: 8FA8F52DFC55D341300EFF8E4C44BA33)
  - wm4J5m8pIK.exe (PID: 5600 cmdline: C:\Users\user\Desktop\wm4J5m8pIK.exe MD5: 8FA8F52DFC55D341300EFF8E4C44BA33)
- dhcpmon.exe (PID: 6316 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 8FA8F52DFC55D341300EFF8E4C44BA33)
  - dhcpmon.exe (PID: 6992 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 8FA8F52DFC55D341300EFF8E4C44BA33)
  - dhcpmon.exe (PID: 7044 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 8FA8F52DFC55D341300EFF8E4C44BA33)
- **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
00000014.00000002.400395562.000000000402 9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000014.00000002.400395562.000000000402 9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x42ee5:$a: NanoCore • 0x42f3e:$a: NanoCore • 0x42f7b:$a: NanoCore • 0x42ff4:$a: NanoCore • 0x5669f:$a: NanoCore • 0x566b4:$a: NanoCore • 0x566e9:$a: NanoCore • 0x6f18b:$a: NanoCore • 0x6f1a0:$a: NanoCore • 0x6f1d5:$a: NanoCore • 0x42f47:$b: ClientPlugin • 0x42f84:$b: ClientPlugin • 0x43882:$b: ClientPlugin • 0x4388f:$b: ClientPlugin • 0x5645b:$b: ClientPlugin • 0x56476:$b: ClientPlugin • 0x564a6:$b: ClientPlugin • 0x566bd:$b: ClientPlugin • 0x566f2:$b: ClientPlugin • 0x6ef47:$b: ClientPlugin • 0x6ef62:$b: ClientPlugin
00000014.00000002.398013426.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000014.00000002.398013426.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000014.00000002.398013426.000000000040 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 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
20.2.dhcpmon.exe.3089658.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
20.2.dhcpmon.exe.3089658.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
20.2.dhcpmon.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
20.2.dhcpmon.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
20.2.dhcpmon.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 14 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 domain / URL
- 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
- 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)

HIPS / PFW / Operating System Protection Evasion:

- .NET source code references suspicious native API functions

Stealing of Sensitive Information:

- Yara detected Nanocore RAT

Remote Access Functionality:

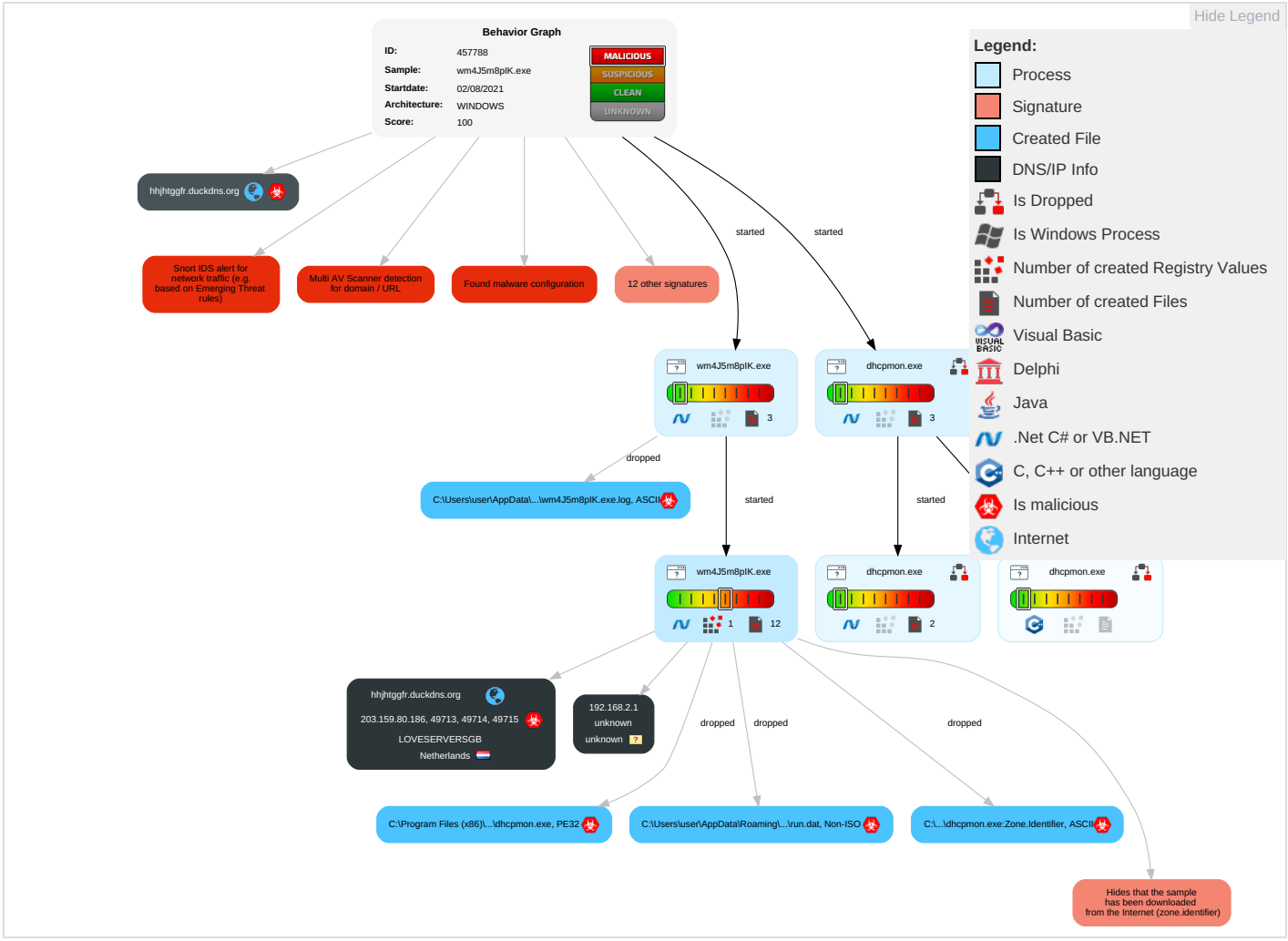
- Detected Nanocore Rat
- Yara detected Nanocore RAT

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 1 1	Query Registry 1	Remote Services	Input Capture 1 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	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exf 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	Exf 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	SIM 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 2	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 Pro

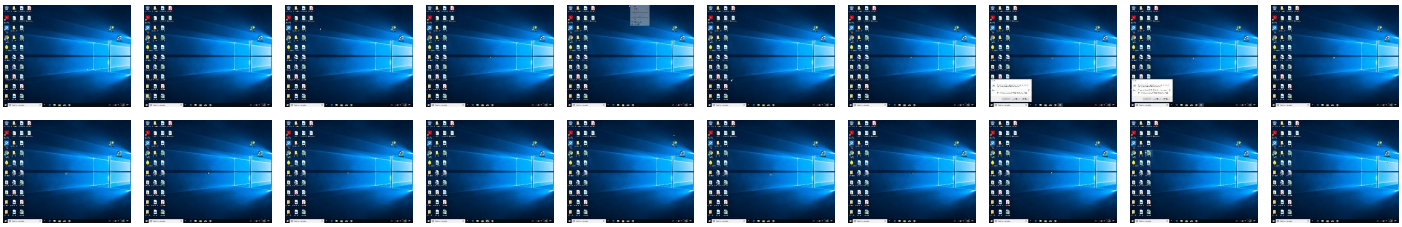
Behavior Graph



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
wm4J5m8pIK.exe	18%	Virustotal		Browse
wm4J5m8pIK.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	18%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
hhjhtggfr.duckdns.org	9%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
hhjhtggfr.duckdns.org	9%	Virustotal		Browse
hhjhtggfr.duckdns.org	0%	Avira URL Cloud	safe	
dertrefg.duckdns.org	8%	Virustotal		Browse
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	• 9%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
hhjhtggfr.duckdns.org	true	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown
dertrefg.duckdns.org	true	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown

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:	457788
Start date:	02.08.2021
Start time:	10:02:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 16s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	wm4J5m8pIK.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@17/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 12% (good quality ratio 12%) • Quality average: 63% • Quality standard deviation: 3.6%
HCA Information:	• Successful, ratio: 99% • 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
10:04:09	API Interceptor	811x Sleep call for process: wm4J5m8pIK.exe modified
10:04:15	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
10:04:53	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	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	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
	MkASxmQIe3.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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	microC.exe	Get hash	malicious	Browse	• 203.159.80.101

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LOVESERVERSGB	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
	g2v7gt7qnt.exe	Get hash	malicious	Browse	• 203.159.80.107
	Pfanner_106888964.exe	Get hash	malicious	Browse	• 203.159.80.182
	THIRD PO.doc	Get hash	malicious	Browse	• 203.159.80.101
	D3NBBjj3lw.exe	Get hash	malicious	Browse	• 203.159.80.101
	iCQfyvJX6i.exe	Get hash	malicious	Browse	• 203.159.80.101
	5iNDenLpgE.exe	Get hash	malicious	Browse	• 203.159.80.101
	zcwuWwArl5.exe	Get hash	malicious	Browse	• 203.159.80.101
	aBV85W9scn.exe	Get hash	malicious	Browse	• 203.159.80.101

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\wm4J5m8pIK.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1378816
Entropy (8bit):	7.548476087877472
Encrypted:	false
SSDEEP:	24576:26IBQ76DOifx8Dgyfx8Dgz06TbTZpq72pMNaDuDHQUl3uwDZzGL:OQ76f58Dgy58Dgz06n1pfWNdlJZa
MD5:	8FA8F52DFC55D341300EFF8E4C44BA33
SHA1:	4FBDB8C39BBC48B159E1F795A2222D51077FDBE9
SHA-256:	2C7DA7FF43C90AE620FD5135C2ED34C7E644A9A1098BFB69F1DC6B8AB6410C9A
SHA-512:	A29B2B8FCDE4EF5917E6AAD29C547D2FCEF3E452B3ED502788BD5BF7CB2E107C46A12783EBBE8EB4AA896C56DFD3FD37C994B67EB5C8F5C9C32FBA75FE48 205
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 18%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...1..a.....P.....L... ...`....@.. .....`..... ..@.....K..O....`.. .....@..... ..... ..H.....text....,... ..... ..`.rsrc... ....`.....0.....@..@.rel oc.....@.....@..B.....K.....H.....0..d.....s.....o.....(....*&..(....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0..... .....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....()....,!r...p....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r1.. p~....o-...(.....t$....+..*...0..&.....(....r7..p~....o-...(.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\wm4J5m8pIK.exe
File Type:	ASCII text, with CRLF line terminators

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
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):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\wm4J5m8pIK.exe.log	
Process:	C:\Users\user\Desktop\wm4J5m8pIK.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\wm4J5m8pIK.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.024371743172393
Encrypted:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCr
MD5:	838CD9DBC78EA45A5406EAE23962086D
SHA1:	C8273AACDEE03AC0CDCDDBAA83F51D04D6A4203C
SHA-256:	6E11A62511C5BBC0413128305069B780C448684B54FAA3E8DD0B4FD3DB8C9867
SHA-512:	F7D25EF1FA6F50667DD6785CC774E0AA6BC52A2231FE96E7C59D14EFDFDDA076F6399288CF6EAC8EFA8A75727893432AA155DA0E392F8CD1F26C5C5871EAC6B5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.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\wm4J5m8pIK.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:TF8t:m
MD5:	E8983D699E232A5B7C1FA96E107D27D4
SHA1:	79C8F3A4338622B7D46DFC878AB52B7AF814D850
SHA-256:	B1024BBCD30F38AB928B05E37771A0F4D2CFA740D301043F787C4C0A99E5F7E5
SHA-512:	68485EFF1C0BDAE02C2F5DC10B18E3AEBA8271C13D2E82E81B5615BD29343CBB1BAB7F4B4E669F94A7FCF6A38D0178E1155D75DC615B560E64148270271A043
Malicious:	**true**
Reputation:	low
Preview:	'.U..U.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\wm4J5m8pIK.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:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671BCB
Malicious:	false
Reputation:	moderate, very likely benign file
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\wm4J5m8pIK.exe
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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
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..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.””.v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[.../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..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):	7.548476087877472
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:	wm4J5m8pIK.exe
File size:	1378816
MD5:	8fa8f52dfc55d341300eff8e4c44ba33
SHA1:	4fbdb8c39bbc48b159e1f795a2222d51077fdbe9
SHA256:	2c7da7ff43c90ae620fd5135c2ed34c7e644a9a1098bfb69f1dc6b8ab6410c9a
SHA512:	a29b2b8fcde4ef5917e6aad29c547d2fcef3e452b3ed502788bd5bf7cb2e107c46a12783ebbe8eb4aa896c56dfd3fd37c994b67eb5c8f5c9c32fba75fe486205
SSDEEP:	24576:26IBQ76DOifx8Dgyfx8Dgz06TbTZpq72pMNaDuDHQUl3uwDZzGL:OQ76f58Dgy58Dgz06n1pfWNdlJZa
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...1..a.....P.....L... ...`....@.. .....`.....@.....

File Icon

Icon Hash:	b07968fcd4ec7090

Static PE Info

General

Entrypoint:	0x544c06
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:	0x61079B31 [Mon Aug 2 07:13:53 2021 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	0x142c0c	0x142e00	False	0.72027136566	data	7.57991184815	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x146000	0xd620	0xd800	False	0.708405671296	data	6.5968021119	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x154000	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
08/02/21-10:04:14.771126	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49713	8234	192.168.2.5	203.159.80.186
08/02/21-10:04:24.339627	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49714	8234	192.168.2.5	203.159.80.186
08/02/21-10:04:29.237612	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49715	8234	192.168.2.5	203.159.80.186
08/02/21-10:04:34.009201	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49717	8234	192.168.2.5	203.159.80.186
08/02/21-10:04:46.937776	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	8234	192.168.2.5	203.159.80.186
08/02/21-10:04:52.000559	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	8234	192.168.2.5	203.159.80.186
08/02/21-10:04:59.132078	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	8234	192.168.2.5	203.159.80.186
08/02/21-10:05:07.264035	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49726	8234	192.168.2.5	203.159.80.186
08/02/21-10:05:12.208710	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	8234	192.168.2.5	203.159.80.186
08/02/21-10:05:18.473782	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	8234	192.168.2.5	203.159.80.186
08/02/21-10:05:27.044328	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49729	8234	192.168.2.5	203.159.80.186
08/02/21-10:05:32.296396	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	8234	192.168.2.5	203.159.80.186
08/02/21-10:05:36.939239	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49734	8234	192.168.2.5	203.159.80.186
08/02/21-10:05:42.049631	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	8234	192.168.2.5	203.159.80.186
08/02/21-10:05:48.052361	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	8234	192.168.2.5	203.159.80.186
08/02/21-10:05:54.013288	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	8234	192.168.2.5	203.159.80.186

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 2, 2021 10:04:14.522439957 CEST	192.168.2.5	8.8.8.8	0x5027	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:04:24.272156000 CEST	192.168.2.5	8.8.8.8	0xe40b	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:04:28.987812042 CEST	192.168.2.5	8.8.8.8	0x745d	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:04:33.680172920 CEST	192.168.2.5	8.8.8.8	0xa0b2	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:04:41.151750088 CEST	192.168.2.5	8.8.8.8	0x167f	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:04:46.871819019 CEST	192.168.2.5	8.8.8.8	0x74c0	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:04:51.942584991 CEST	192.168.2.5	8.8.8.8	0x92dd	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:04:59.064100981 CEST	192.168.2.5	8.8.8.8	0x6414	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:07.196168900 CEST	192.168.2.5	8.8.8.8	0x8f43	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:12.152043104 CEST	192.168.2.5	8.8.8.8	0x1cca	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:18.252171040 CEST	192.168.2.5	8.8.8.8	0x7699	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:26.979337931 CEST	192.168.2.5	8.8.8.8	0x9fa5	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:32.083272934 CEST	192.168.2.5	8.8.8.8	0xf87d	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:36.863857985 CEST	192.168.2.5	8.8.8.8	0xa636	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:41.977792025 CEST	192.168.2.5	8.8.8.8	0xc297	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:47.985821962 CEST	192.168.2.5	8.8.8.8	0x9f9f	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:53.946765900 CEST	192.168.2.5	8.8.8.8	0x78f2	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 2, 2021 10:04:14.662118912 CEST	8.8.8.8	192.168.2.5	0x5027	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:04:24.308578014 CEST	8.8.8.8	192.168.2.5	0xe40b	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:04:29.022208929 CEST	8.8.8.8	192.168.2.5	0x745d	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:04:33.817778111 CEST	8.8.8.8	192.168.2.5	0xa0b2	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:04:41.187736034 CEST	8.8.8.8	192.168.2.5	0x167f	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:04:46.904643059 CEST	8.8.8.8	192.168.2.5	0x74c0	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:04:51.970065117 CEST	8.8.8.8	192.168.2.5	0x92dd	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:04:59.097481012 CEST	8.8.8.8	192.168.2.5	0x6414	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:07.231401920 CEST	8.8.8.8	192.168.2.5	0x8f43	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:12.177535057 CEST	8.8.8.8	192.168.2.5	0x1cca	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:18.390911102 CEST	8.8.8.8	192.168.2.5	0x7699	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 2, 2021 10:05:27.007220984 CEST	8.8.8.8	192.168.2.5	0x9fa5	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:32.221256018 CEST	8.8.8.8	192.168.2.5	0xf87d	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:36.898267031 CEST	8.8.8.8	192.168.2.5	0xa636	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:42.014321089 CEST	8.8.8.8	192.168.2.5	0xc297	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:48.019078016 CEST	8.8.8.8	192.168.2.5	0x9f9f	No error (0)	hhjhtggfr.duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:05:53.982575893 CEST	8.8.8.8	192.168.2.5	0x78f2	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: wm4J5m8pIK.exe PID: 5804 Parent PID: 5732

General

Start time:	10:03:45
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\wm4J5m8pIK.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\wm4J5m8pIK.exe'
Imagebase:	0x660000
File size:	1378816 bytes
MD5 hash:	8FA8F52DFC55D341300EFF8E4C44BA33
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 Written

File Read

Analysis Process: wm4J5m8pIK.exe PID: 5600 Parent PID: 5804

General

Start time:	10:04:10
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\wm4J5m8pIK.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\wm4J5m8pIK.exe
Imagebase:	0x460000
File size:	1378816 bytes
MD5 hash:	8FA8F52DFC55D341300EFF8E4C44BA33
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: 6316 Parent PID: 3472

General

Start time:	10:04:24
Start date:	02/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xa0000
File size:	1378816 bytes
MD5 hash:	8FA8F52DFC55D341300EFF8E4C44BA33
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 18%, Virustotal, Browse
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 6992 Parent PID: 6316

General

Start time:	10:04:54
Start date:	02/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x3a0000
File size:	1378816 bytes
MD5 hash:	8FA8F52DFC55D341300EFF8E4C44BA33
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: 7044 Parent PID: 6316

General

Start time:	10:04:55
Start date:	02/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x820000
File size:	1378816 bytes
MD5 hash:	8FA8F52DFC55D341300EFF8E4C44BA33
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: 00000014.00000002.400395562.0000000004029000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.400395562.0000000004029000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.398013426.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.398013426.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.398013426.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.400062984.0000000003021000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.400062984.0000000003021000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis