ID: 452025
Sample Name: yMI7.exe
Cookbook: default.jbs
Time: 18:08:08
Date: 21/07/2021
Version: 33.0.0 White Diamond

Table of Contents

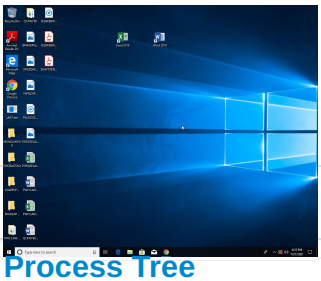
Windows Analysis Report yMI7.exe

Overview

General Information

Sample Name:	yMI7.exe
Analysis ID:	452025
MD5:	39121091956f893.
SHA1:	2d63ef96343bd46.
SHA256:	9a2247160056d9..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

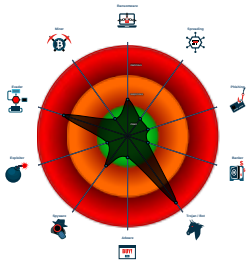
Nanocore

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- 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 Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w10x64**
- yMI7.exe (PID: 784 cmdline: 'C:\Users\user\Desktop\yMI7.exe' MD5: 39121091956F8934B1C73041EE1CC90F)
- dhcpmon.exe (PID: 4188 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 39121091956F8934B1C73041EE1CC90F)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "1d151c9c-8c5a-49a2-b97c-b83e2e70",
  "Group": "Default",
  "Domain1": "marquinhos-36228.portmap.host",
  "Domain2": "127.0.0.1",
  "Port": 36228,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
yMI7.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
yMI7.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
yMI7.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
yMI7.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.234012520.000000000722000.00000002.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000005.00000000.234012520.000000000722000.00000002.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000005.00000000.234012520.000000000722000.00000002.00020000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000005.00000002.251432444.000000000722000.00000002.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000005.00000002.251432444.000000000722000.00000002.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.dhcpmon.exe.2e68e2c.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
5.2.dhcpmon.exe.2e68e2c.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated
5.2.dhcpmon.exe.3f5a5aa.7.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
5.2.dhcpmon.exe.3f5a5aa.7.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated

Source	Rule	Description	Author	Strings
5.2.dhcpmon.exe.3f667dc.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
Click to see the 29 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:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

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

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

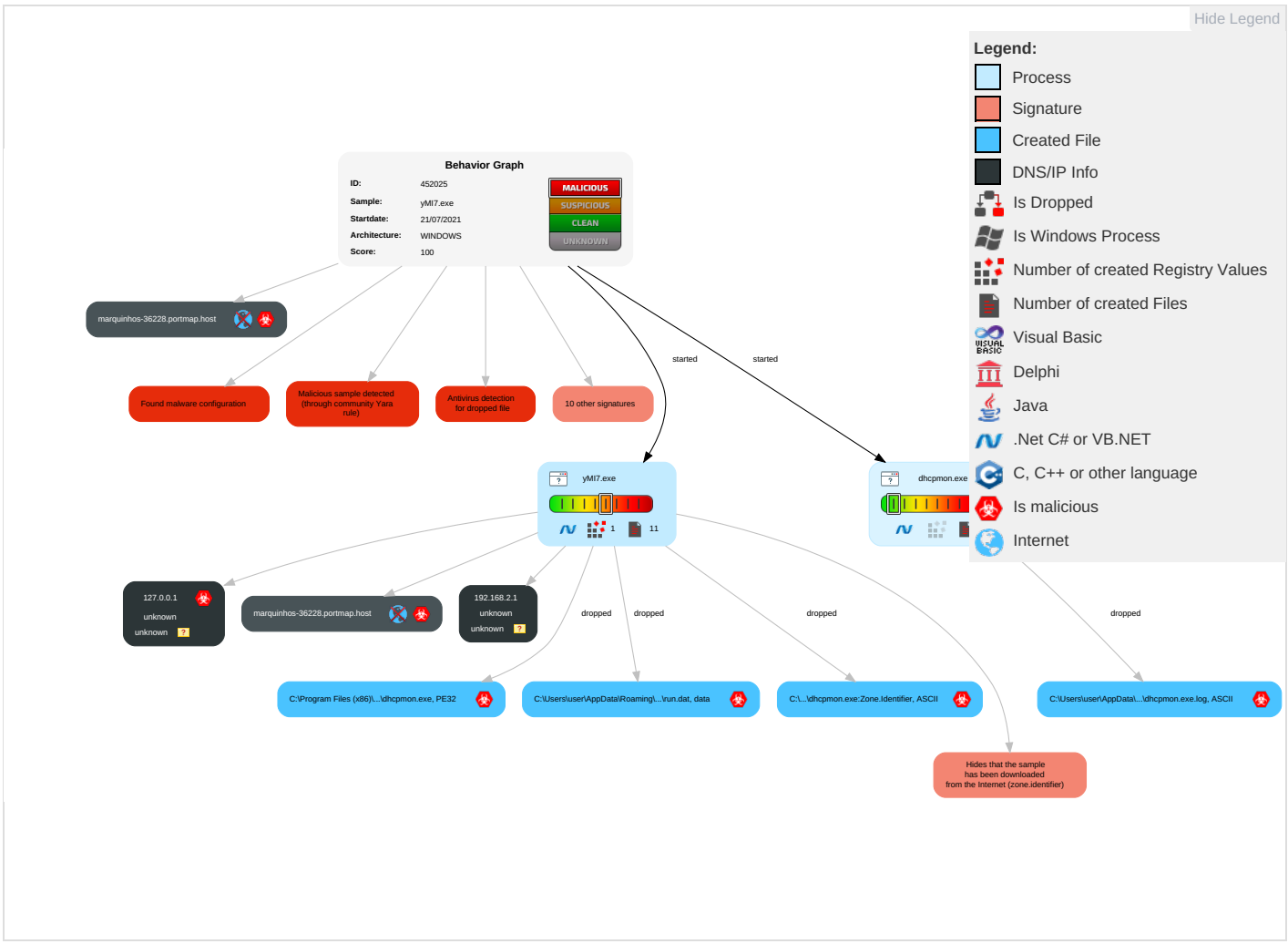
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

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

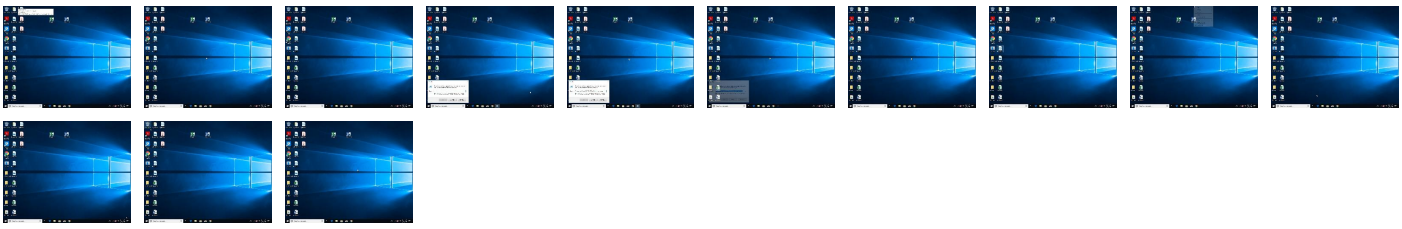
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
yMI7.exe	80%	Virustotal		Browse
yMI7.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
yMI7.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	80%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.yMI7.exe.ba0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.dhcpmon.exe.720000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.dhcpmon.exe.720000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
marquinhos-36228.portmap.host	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Virustotal		Browse
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
marquinhos-36228.portmap.host	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
marquinhos-36228.portmap.host	true	• Avira URL Cloud: safe	unknown
127.0.0.1	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452025
Start date:	21.07.2021
Start time:	18:08:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	yMI7.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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.evad.winEXE@2/4@45/2
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
18:08:56	API Interceptor	1059x Sleep call for process: yMI7.exe modified
18:09:01	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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\yMI7.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	486400
Entropy (8bit):	7.858767992660797
Encrypted:	false
SSDEEP:	12288:MLV6BtpmkSYu1kSk63qiwi1kdENzqCm1zTZsiqx60HidcAEx43y:+ApfSYu+r6YSkdE5mFTZ+Hq243y
MD5:	39121091956F8934B1C73041EE1CC90F
SHA1:	2D63EF96343BD4636CED243F81CE9CC361B28F74
SHA-256:	9A2247160056D9A5DE43A34672B7E1650402A8EC6F435F1EF0D07A5347907404

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
SHA-512:	83671F6DFFBB90B6DDBE7504E9805AA5A66E8FD8025B3B8C330A37CF342F845F880B0A9A6ED95BE70F1A5FE0994FD3B6A4E8C4BDBE59ADD0183DBAD95A7CE8FC
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 80%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T..... .....@.. .....8...W.... ....H.....text..... ....`.reloc.....@..B.rsrc..... .....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$.....~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\yMI7.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\yMI7.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:Hilp8t:LSt
MD5:	D968E8CAF6CE7C3F89D60D184D89ECCB
SHA1:	9EE5ADC2852A7FBF89475B4DA612C1F601B4FB99
SHA-256:	406646F65342BC1D184FB76057FDFC62ED701E62E2696709F5C249B720BED595
SHA-512:	88D7E0046B9D109DB70858AEC41F0971F9F0A80207539B6B51C4892971DC381F3F3E933A075D01F87B8C8F5B9736F6BE9749BF2BD27F58DD011BCCC9E4FC513
Malicious:	**true**

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Reputation:	low
Preview:	...G.L.H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.858767992660797
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:	yMI7.exe
File size:	486400
MD5:	39121091956f8934b1c73041ee1cc90f
SHA1:	2d63ef96343bd4636ced243f81ce9cc361b28f74
SHA256:	9a2247160056d9a5de43a34672b7e1650402a8ec6f435f1ef0d07a5347907404
SHA512:	83671f6dffbb90b6ddbe7504e9805aa5a66e8fd8025b3b8c330a37cf342f845f880b0a9a6ed95be70f1a5fe0994fd3b6a4e8c4bdbe59add0183dbad95a7ce8fc
SSDEEP:	12288:MLV6BtpmkSYu1kSk63qiwi1kdENzqCm1zTZsiqx60HidcAEx43y:+ApfSYu+r6YSkdE5mFTZ+Hq243y
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T..... .....@.. ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

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

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1c798	0x1c800	False	0.594503837719	data	6.59807609597	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x59e18	0x5a000	False	0.999126519097	data	7.99949505545	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2021 18:08:59.154131889 CEST	192.168.2.3	8.8.8.8	0x7d2	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:08:59.234327078 CEST	192.168.2.3	8.8.4.4	0x9d21	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:08:59.265060902 CEST	192.168.2.3	8.8.8.8	0x65d	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:03.390698910 CEST	192.168.2.3	8.8.8.8	0xff3e	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:03.433067083 CEST	192.168.2.3	8.8.4.4	0x776	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:03.454628944 CEST	192.168.2.3	8.8.8.8	0xbfcc	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:07.606671095 CEST	192.168.2.3	8.8.8.8	0xe9c2	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:07.711667061 CEST	192.168.2.3	8.8.4.4	0x1659	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:07.798871040 CEST	192.168.2.3	8.8.8.8	0x2a7	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:27.610974073 CEST	192.168.2.3	8.8.8.8	0x4ee9	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:27.628843069 CEST	192.168.2.3	8.8.4.4	0x1d6e	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:27.827480078 CEST	192.168.2.3	8.8.8.8	0x7352	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:31.936835051 CEST	192.168.2.3	8.8.8.8	0x54b5	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:31.953711987 CEST	192.168.2.3	8.8.4.4	0x3d0e	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2021 18:09:31.975235939 CEST	192.168.2.3	8.8.8.8	0x1906	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:36.034465075 CEST	192.168.2.3	8.8.8.8	0x875	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:36.050039053 CEST	192.168.2.3	8.8.4.4	0xd11c	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:36.069166899 CEST	192.168.2.3	8.8.8.8	0xbff	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:55.256452084 CEST	192.168.2.3	8.8.8.8	0xea5	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:55.300771952 CEST	192.168.2.3	8.8.4.4	0xa266	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:55.320933104 CEST	192.168.2.3	8.8.8.8	0x2cc5	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:59.371862888 CEST	192.168.2.3	8.8.8.8	0x93ee	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:59.523283958 CEST	192.168.2.3	8.8.4.4	0x9120	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:59.544392109 CEST	192.168.2.3	8.8.8.8	0xb47d	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:03.617001057 CEST	192.168.2.3	8.8.8.8	0x61b	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:03.718733072 CEST	192.168.2.3	8.8.4.4	0xf2af	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:03.884324074 CEST	192.168.2.3	8.8.8.8	0xd41f	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:23.072074890 CEST	192.168.2.3	8.8.8.8	0xe1b4	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:23.088762999 CEST	192.168.2.3	8.8.4.4	0x802d	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:23.119174957 CEST	192.168.2.3	8.8.8.8	0x9fff	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:27.210969925 CEST	192.168.2.3	8.8.8.8	0x47c9	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:27.227534056 CEST	192.168.2.3	8.8.4.4	0xb168	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:27.246526957 CEST	192.168.2.3	8.8.8.8	0x735e	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:31.314162016 CEST	192.168.2.3	8.8.8.8	0x5f8f	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:31.333368063 CEST	192.168.2.3	8.8.4.4	0x9f83	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:31.361603975 CEST	192.168.2.3	8.8.8.8	0xa6d0	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:50.875526905 CEST	192.168.2.3	8.8.8.8	0xb830	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:50.915549994 CEST	192.168.2.3	8.8.4.4	0xef2a	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:50.934480906 CEST	192.168.2.3	8.8.8.8	0x3da4	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:54.999332905 CEST	192.168.2.3	8.8.8.8	0x5778	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2021 18:10:55.019088030 CEST	192.168.2.3	8.8.4.4	0x37c1	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:55.068900108 CEST	192.168.2.3	8.8.8.8	0xba8f	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:59.121402979 CEST	192.168.2.3	8.8.8.8	0x575b	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:59.137598991 CEST	192.168.2.3	8.8.4.4	0xe731	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:59.164417982 CEST	192.168.2.3	8.8.8.8	0x9055	Standard query (0)	marquinhos-36228.portmap.host	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2021 18:08:59.189044952 CEST	8.8.8.8	192.168.2.3	0x7d2	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:08:59.248064995 CEST	8.8.4.4	192.168.2.3	0x9d21	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:08:59.278369904 CEST	8.8.8.8	192.168.2.3	0x65d	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:03.404673100 CEST	8.8.8.8	192.168.2.3	0xff3e	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:03.446898937 CEST	8.8.4.4	192.168.2.3	0x776	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:03.468732119 CEST	8.8.8.8	192.168.2.3	0xbfcc	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:07.620855093 CEST	8.8.8.8	192.168.2.3	0xe9c2	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:07.724493980 CEST	8.8.4.4	192.168.2.3	0x1659	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:07.812117100 CEST	8.8.8.8	192.168.2.3	0x2a7	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:27.625359058 CEST	8.8.8.8	192.168.2.3	0x4ee9	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:27.642312050 CEST	8.8.4.4	192.168.2.3	0x1d6e	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:27.840261936 CEST	8.8.8.8	192.168.2.3	0x7352	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:31.950519085 CEST	8.8.8.8	192.168.2.3	0x54b5	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:31.967222929 CEST	8.8.4.4	192.168.2.3	0x3d0e	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:31.988960028 CEST	8.8.8.8	192.168.2.3	0x1906	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:36.047396898 CEST	8.8.8.8	192.168.2.3	0x875	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:36.063028097 CEST	8.8.4.4	192.168.2.3	0xd11c	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:36.082801104 CEST	8.8.8.8	192.168.2.3	0xbff	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:55.269335985 CEST	8.8.8.8	192.168.2.3	0xea5	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2021 18:09:55.314256907 CEST	8.8.4.4	192.168.2.3	0xa266	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:55.334157944 CEST	8.8.8.8	192.168.2.3	0x2cc5	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:59.384891987 CEST	8.8.8.8	192.168.2.3	0x93ee	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:59.538171053 CEST	8.8.4.4	192.168.2.3	0x9120	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:09:59.559184074 CEST	8.8.8.8	192.168.2.3	0xb47d	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:03.630134106 CEST	8.8.8.8	192.168.2.3	0x61b	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:03.733841896 CEST	8.8.4.4	192.168.2.3	0xf2af	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:03.898324013 CEST	8.8.8.8	192.168.2.3	0xd41f	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:23.085443020 CEST	8.8.8.8	192.168.2.3	0xe1b4	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:23.102976084 CEST	8.8.4.4	192.168.2.3	0x802d	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:23.133109093 CEST	8.8.8.8	192.168.2.3	0x9fff	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:27.224175930 CEST	8.8.8.8	192.168.2.3	0x47c9	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:27.239530087 CEST	8.8.4.4	192.168.2.3	0xb168	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:27.259665012 CEST	8.8.8.8	192.168.2.3	0x735e	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:31.327352047 CEST	8.8.8.8	192.168.2.3	0x5f8f	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:31.346574068 CEST	8.8.4.4	192.168.2.3	0x9f83	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:31.374669075 CEST	8.8.8.8	192.168.2.3	0xa6d0	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:50.889142036 CEST	8.8.8.8	192.168.2.3	0xb830	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:50.928364038 CEST	8.8.4.4	192.168.2.3	0xef2a	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:50.948419094 CEST	8.8.8.8	192.168.2.3	0x3da4	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:55.013149977 CEST	8.8.8.8	192.168.2.3	0x5778	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:55.031843901 CEST	8.8.4.4	192.168.2.3	0x37c1	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:55.083175898 CEST	8.8.8.8	192.168.2.3	0xba8f	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:59.134984970 CEST	8.8.8.8	192.168.2.3	0x575b	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:59.150541067 CEST	8.8.4.4	192.168.2.3	0xe731	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 18:10:59.177824974 CEST	8.8.8.8	192.168.2.3	0x9055	Name error (3)	marquinhos-36228.portmap.host	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: yMI7.exe PID: 784 Parent PID: 5664

General

Start time:	18:08:55
Start date:	21/07/2021
Path:	C:\Users\user\Desktop\yMI7.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\yMI7.exe'
Imagebase:	0xba0000
File size:	486400 bytes
MD5 hash:	39121091956F8934B1C73041EE1CC90F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000000.203043099.0000000000BA2000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.203043099.0000000000BA2000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.203043099.0000000000BA2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: dhcpmon.exe PID: 4188 Parent PID: 3388

General

Start time:	18:09:09
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:	0x720000
File size:	486400 bytes
MD5 hash:	39121091956F8934B1C73041EE1CC90F
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: 00000005.00000000.234012520.0000000000722000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.234012520.0000000000722000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.234012520.0000000000722000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.251432444.0000000000722000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.251432444.0000000000722000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.251432444.0000000000722000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.252582895.0000000003E41000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.252582895.0000000003E41000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.252465646.0000000002E41000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.252465646.0000000002E41000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 80%, Virustotal, Browse
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis