ID: 452192
Sample Name: TRwrC.exe
Cookbook: default.jbs
Time: 23:08:11
Date: 21/07/2021
Version: 33.0.0 White Diamond

Table of Contents

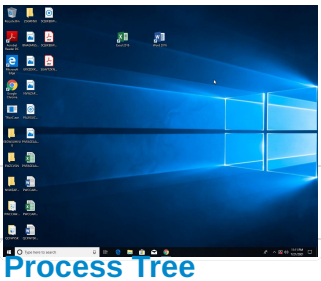
Windows Analysis Report TRwrC.exe

Overview

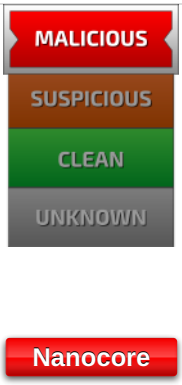
General Information

Sample Name:	TRwrC.exe
Analysis ID:	452192
MD5:	eaa9755979d4ed..
SHA1:	0ba5fc95f551f89…
SHA256:	6f6d5cffc1e9278…
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

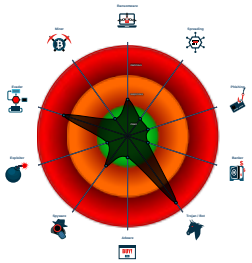


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 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…
- Machine Learning detection for dropp…

Classification



Process Tree

- **System is w10x64**
- TRwrC.exe (PID: 2044 cmdline: 'C:\Users\user\Desktop\TRwrC.exe' MD5: EAA9755979D4EDEAC9C48FFB1F42551C)
- dhcpmon.exe (PID: 5876 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: EAA9755979D4EDEAC9C48FFB1F42551C)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "e8dbb34a-f657-4ae4-ba56-6d78335a",
  "Group": "Minecraft SMP10PC",
  "Domain1": "domingos-50227.portmap.io",
  "Domain2": "domingos-50227.portmap.io",
  "Port": 50227,
  "KeyboardLogging": "Disable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Enable",
  "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
TRwrC.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
TRwrC.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
TRwrC.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
TRwrC.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
00000005.00000000.233225156.0000000000D2 2000.00000002.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000005.00000000.233225156.0000000000D2 2000.00000002.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000005.00000000.233225156.0000000000D2 2000.00000002.00020000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000005.00000002.248661530.0000000000D2 2000.00000002.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000005.00000002.248661530.0000000000D2 2000.00000002.00020000.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.34f3dc4.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
5.2.dhcpmon.exe.34f3dc4.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
0.0.TRwrC.exe.460000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.0.TRwrC.exe.460000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
0.0.TRwrC.exe.460000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 22 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 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:

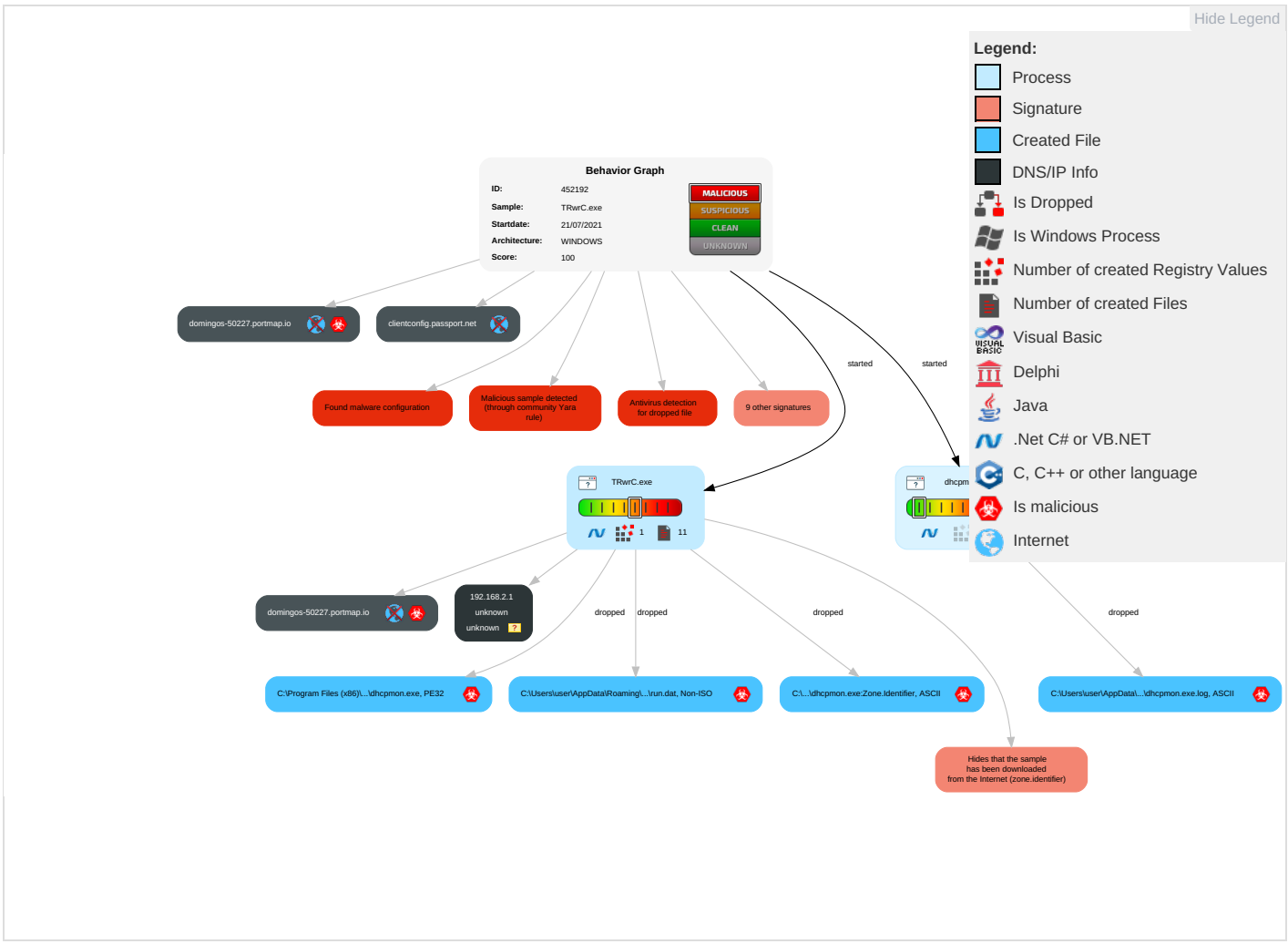
Detected Nanocore Rat

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 1	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 1	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 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 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 1	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

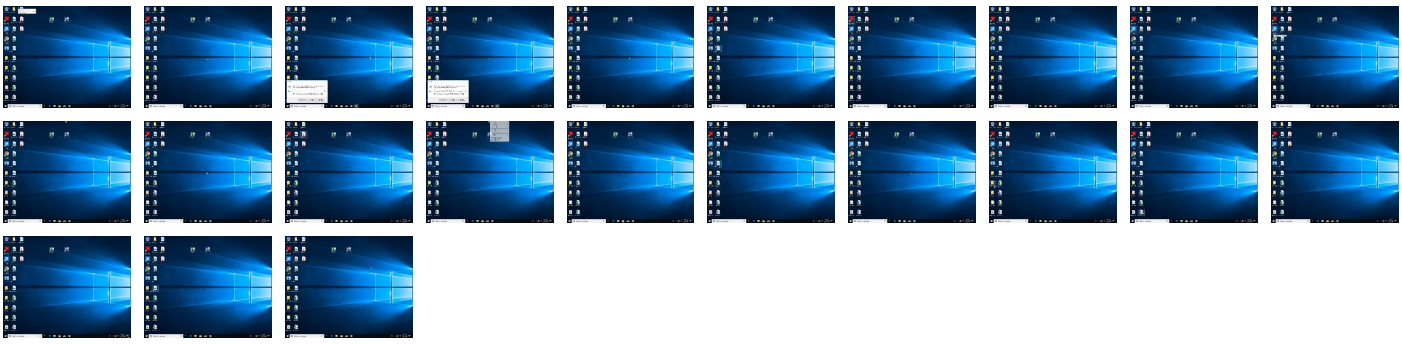
Behavior Graph



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
TRwrC.exe	80%	Virustotal		Browse
TRwrC.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
TRwrC.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		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.dhcpmon.exe.d20000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.0.TRwrC.exe.460000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.dhcpmon.exe.d20000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
clientconfig.passport.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
domingos-50227.portmap.io	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
domingos-50227.portmap.io	unknown	unknown	true		unknown
clientconfig.passport.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
domingos-50227.portmap.io	true	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452192
Start date:	21.07.2021
Start time:	23:08:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TRwrC.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:	22
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@85/1
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
23:09:01	API Interceptor	1035x Sleep call for process: TRwrC.exe modified
23:09:05	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\TRwrC.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207360
Entropy (8bit):	7.4462121180145955
Encrypted:	false
SSDEEP:	6144:wLV6Bta6dtJmakIM5EP5BqF9aK4qzdbmrcPSJ:wLV6BtpmkXBBq/aK4qzdgJ
MD5:	EAA9755979D4EDEAC9C48FFB1F42551C
SHA1:	0BA5FC95F551F89648E0DDAE327E60FFA417712F
SHA-256:	6F6D5CFFC1E927811613347C2C10F9071434FEDDE5780114089981E494B573A7
SHA-512:	37FC60D70C6E573EF2FF1CBDC984614E6ECECBEE34966FB11D21703B222A3D32D64F2D519B4617C2C33AB5AD81A60FCF65E8D39AB62C145A070657D94918BEA
Malicious:	**true**

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
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%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. ..... .....8...W.... ...]..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc....]... ...^.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s 8....-&&s9....,$&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\TRwrC.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_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\TRwrC.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:G8t:G8t
MD5:	17DF4C94B762C5452096EEE6EA66B7A2
SHA1:	B7A1FE5F514EBC025C887F1B6D5BA487571C4194
SHA-256:	D1188FFBAE4C49985758F21568E408700F8B7F43E769181C1477CA8C07571271
SHA-512:	42704F70997DBF94EF892B010D03E517482237063B0188766F663181575AFA552B0B7C32BE2624A854A3E3344D089865D36A3EF3248D6E71DF8A0E7507DE768A
Malicious:	**true**
Reputation:	low
Preview:	..3.L.H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.4462121180145955
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:	TRwrC.exe
File size:	207360
MD5:	eaa9755979d4edeac9c48ffb1f42551c
SHA1:	0ba5fc95f551f89648e0ddae327e60ffa417712f
SHA256:	6f6d5cffc1e927811613347c2c10f9071434fedde5780114089981e494b573a7
SHA512:	37fc60d70c6e573ef2ff1cbdc984614e6ececbee34966fb11d21703b222a3d32d64f2d519b4617c2c33ab5ad81a60fcf65e8d39ab62c145a070657d94918beda
SSDEEP:	6144:wLV6Bta6dtJmakIM5EP5BqF9aK4qzdbmrcPSJ:wLV6BtpmkXBBq/aK4qzdgJ
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	6.59805919516	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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	0x15d98	0x15e00	False	0.999765625	data	7.99761824146	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 23:08:53.093976974 CEST	192.168.2.3	8.8.8.8	0xdfcf	Standard query (0)	clientconfig.passport.net	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:03.011032104 CEST	192.168.2.3	8.8.8.8	0x69fa	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:03.097588062 CEST	192.168.2.3	8.8.4.4	0x2425	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:03.250005007 CEST	192.168.2.3	8.8.8.8	0x4c30	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:07.346379995 CEST	192.168.2.3	8.8.8.8	0xc60b	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:07.371016026 CEST	192.168.2.3	8.8.4.4	0xbabe	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:07.402482033 CEST	192.168.2.3	8.8.8.8	0xebb6	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:11.472805023 CEST	192.168.2.3	8.8.8.8	0xf314	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:11.528441906 CEST	192.168.2.3	8.8.4.4	0x9d26	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:11.599323034 CEST	192.168.2.3	8.8.8.8	0xb4ba	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:15.702580929 CEST	192.168.2.3	8.8.8.8	0xb08a	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:15.726527929 CEST	192.168.2.3	8.8.4.4	0xbab	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:15.755559921 CEST	192.168.2.3	8.8.8.8	0xb8c1	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:19.825299025 CEST	192.168.2.3	8.8.8.8	0xa923	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:19.850053072 CEST	192.168.2.3	8.8.4.4	0x4404	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:19.877332926 CEST	192.168.2.3	8.8.8.8	0x7228	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:23.963464975 CEST	192.168.2.3	8.8.8.8	0x800b	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:23.998766899 CEST	192.168.2.3	8.8.4.4	0x6e27	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:24.060472965 CEST	192.168.2.3	8.8.8.8	0x3a10	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:28.165015936 CEST	192.168.2.3	8.8.8.8	0x2761	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:28.190262079 CEST	192.168.2.3	8.8.4.4	0x1371	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:28.258061886 CEST	192.168.2.3	8.8.8.8	0x8b80	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:32.329732895 CEST	192.168.2.3	8.8.8.8	0xf2fb	Standard query (0)	domingos-50227.portmap.io	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2021 23:09:33.341167927 CEST	192.168.2.3	8.8.8.8	0xf2fb	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:34.341768026 CEST	192.168.2.3	8.8.8.8	0xf2fb	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:36.564687967 CEST	192.168.2.3	8.8.8.8	0xf2fb	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:40.607577085 CEST	192.168.2.3	8.8.8.8	0xf2fb	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:44.785906076 CEST	192.168.2.3	8.8.4.4	0x3910	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:45.795742989 CEST	192.168.2.3	8.8.4.4	0x3910	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:46.841794968 CEST	192.168.2.3	8.8.4.4	0x3910	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:48.873285055 CEST	192.168.2.3	8.8.4.4	0x3910	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:48.934243917 CEST	192.168.2.3	8.8.8.8	0x5a51	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:53.417315006 CEST	192.168.2.3	8.8.8.8	0xe61d	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:53.482561111 CEST	192.168.2.3	8.8.4.4	0x4528	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:53.511677980 CEST	192.168.2.3	8.8.8.8	0xc8de	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:57.737369061 CEST	192.168.2.3	8.8.8.8	0x5b01	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:57.764597893 CEST	192.168.2.3	8.8.4.4	0x19e5	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:57.795141935 CEST	192.168.2.3	8.8.8.8	0x7942	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:01.856786013 CEST	192.168.2.3	8.8.8.8	0x1491	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:01.884063959 CEST	192.168.2.3	8.8.4.4	0xabf	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:01.946635008 CEST	192.168.2.3	8.8.8.8	0x3e8c	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:06.039859056 CEST	192.168.2.3	8.8.8.8	0x7f38	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:06.091521978 CEST	192.168.2.3	8.8.4.4	0x6e91	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:06.130650997 CEST	192.168.2.3	8.8.8.8	0x5c91	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:10.255323887 CEST	192.168.2.3	8.8.8.8	0x5bfc	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:10.283751011 CEST	192.168.2.3	8.8.4.4	0x6edd	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:10.318248987 CEST	192.168.2.3	8.8.8.8	0x7e4f	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:14.377334118 CEST	192.168.2.3	8.8.8.8	0xe54	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:15.391719103 CEST	192.168.2.3	8.8.8.8	0xe54	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:16.423003912 CEST	192.168.2.3	8.8.8.8	0xe54	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:18.428855896 CEST	192.168.2.3	8.8.8.8	0xe54	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:22.443547964 CEST	192.168.2.3	8.8.8.8	0xe54	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:26.612273932 CEST	192.168.2.3	8.8.4.4	0x1112	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:27.654588938 CEST	192.168.2.3	8.8.4.4	0x1112	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:28.764767885 CEST	192.168.2.3	8.8.4.4	0x1112	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:30.994569063 CEST	192.168.2.3	8.8.4.4	0x1112	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:35.037904024 CEST	192.168.2.3	8.8.4.4	0x1112	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:35.256297112 CEST	192.168.2.3	8.8.8.8	0x7713	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:39.367691040 CEST	192.168.2.3	8.8.8.8	0x1ea7	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:39.399648905 CEST	192.168.2.3	8.8.4.4	0x108c	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2021 23:10:39.491625071 CEST	192.168.2.3	8.8.8.8	0xec2f	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:43.567359924 CEST	192.168.2.3	8.8.8.8	0x10c3	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:43.597448111 CEST	192.168.2.3	8.8.4.4	0x8a08	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:43.663613081 CEST	192.168.2.3	8.8.8.8	0x3f28	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:47.740528107 CEST	192.168.2.3	8.8.8.8	0xbb44	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:47.771562099 CEST	192.168.2.3	8.8.4.4	0x36de	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:47.808650017 CEST	192.168.2.3	8.8.8.8	0x4651	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:51.890292883 CEST	192.168.2.3	8.8.8.8	0x1e9c	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:51.961401939 CEST	192.168.2.3	8.8.4.4	0x2ee5	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:51.999831915 CEST	192.168.2.3	8.8.8.8	0xf023	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:56.074913979 CEST	192.168.2.3	8.8.8.8	0x8915	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:56.105568886 CEST	192.168.2.3	8.8.4.4	0xa297	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:56.140166044 CEST	192.168.2.3	8.8.8.8	0x1bbf	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:00.387906075 CEST	192.168.2.3	8.8.8.8	0x7fb6	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:00.415723085 CEST	192.168.2.3	8.8.4.4	0xdbfb	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:00.449387074 CEST	192.168.2.3	8.8.8.8	0x52c7	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:04.524609089 CEST	192.168.2.3	8.8.8.8	0xda29	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:04.587970972 CEST	192.168.2.3	8.8.4.4	0xf82d	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:04.622313976 CEST	192.168.2.3	8.8.8.8	0xc664	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:08.679136992 CEST	192.168.2.3	8.8.8.8	0xfa5d	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:08.705286980 CEST	192.168.2.3	8.8.4.4	0x4447	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:08.734215975 CEST	192.168.2.3	8.8.8.8	0xb0e8	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:12.772248030 CEST	192.168.2.3	8.8.8.8	0x41ac	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:12.803313971 CEST	192.168.2.3	8.8.4.4	0xb4e5	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:12.838100910 CEST	192.168.2.3	8.8.8.8	0x8f5e	Standard query (0)	domingos-5 0227.portmap.io	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2021 23:08:52.902782917 CEST	8.8.8.8	192.168.2.3	0x9cb	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 23:08:53.148514032 CEST	8.8.8.8	192.168.2.3	0xdfcf	No error (0)	clientconfig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 23:09:03.037568092 CEST	8.8.8.8	192.168.2.3	0x69fa	Name error (3)	domingos-5 0227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:03.121460915 CEST	8.8.4.4	192.168.2.3	0x2425	Name error (3)	domingos-5 0227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:03.270798922 CEST	8.8.8.8	192.168.2.3	0x4c30	Name error (3)	domingos-5 0227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:07.367633104 CEST	8.8.8.8	192.168.2.3	0xc60b	Name error (3)	domingos-5 0227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:07.392586946 CEST	8.8.4.4	192.168.2.3	0xbabe	Name error (3)	domingos-5 0227.portmap.io	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2021 23:09:07.424400091 CEST	8.8.8.8	192.168.2.3	0xebb6	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:11.494216919 CEST	8.8.8.8	192.168.2.3	0xf314	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:11.550044060 CEST	8.8.4.4	192.168.2.3	0x9d26	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:11.622447968 CEST	8.8.8.8	192.168.2.3	0xb4ba	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:15.723352909 CEST	8.8.8.8	192.168.2.3	0xb08a	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:15.749783039 CEST	8.8.4.4	192.168.2.3	0xbab	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:15.777122974 CEST	8.8.8.8	192.168.2.3	0xb8c1	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:19.846515894 CEST	8.8.8.8	192.168.2.3	0xa923	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:19.871386051 CEST	8.8.4.4	192.168.2.3	0x4404	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:19.898648977 CEST	8.8.8.8	192.168.2.3	0x7228	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:23.994505882 CEST	8.8.8.8	192.168.2.3	0x800b	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:24.019367933 CEST	8.8.4.4	192.168.2.3	0x6e27	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:24.083601952 CEST	8.8.8.8	192.168.2.3	0x3a10	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:28.187236071 CEST	8.8.8.8	192.168.2.3	0x2761	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:28.211791992 CEST	8.8.4.4	192.168.2.3	0x1371	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:28.279025078 CEST	8.8.8.8	192.168.2.3	0x8b80	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:48.895234108 CEST	8.8.4.4	192.168.2.3	0x3910	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:48.957051039 CEST	8.8.8.8	192.168.2.3	0x5a51	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:53.439857006 CEST	8.8.8.8	192.168.2.3	0xe61d	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:53.504436016 CEST	8.8.4.4	192.168.2.3	0x4528	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:53.534105062 CEST	8.8.8.8	192.168.2.3	0xc8de	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:57.760548115 CEST	8.8.8.8	192.168.2.3	0x5b01	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:57.788250923 CEST	8.8.4.4	192.168.2.3	0x19e5	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:09:57.819818020 CEST	8.8.8.8	192.168.2.3	0x7942	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:01.880403042 CEST	8.8.8.8	192.168.2.3	0x1491	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:01.907223940 CEST	8.8.4.4	192.168.2.3	0xabf	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)

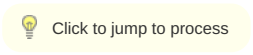
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2021 23:10:01.968517065 CEST	8.8.8.8	192.168.2.3	0x3e8c	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:06.060714006 CEST	8.8.8.8	192.168.2.3	0x7f38	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:06.111661911 CEST	8.8.4.4	192.168.2.3	0x6e91	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:06.155224085 CEST	8.8.8.8	192.168.2.3	0x5c91	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:10.276299953 CEST	8.8.8.8	192.168.2.3	0x5bfc	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:10.306091070 CEST	8.8.4.4	192.168.2.3	0x6edd	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:10.339683056 CEST	8.8.8.8	192.168.2.3	0x7e4f	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:35.066896915 CEST	8.8.4.4	192.168.2.3	0x1112	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:35.285720110 CEST	8.8.8.8	192.168.2.3	0x7713	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:39.393793106 CEST	8.8.8.8	192.168.2.3	0x1ea7	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:39.424127102 CEST	8.8.4.4	192.168.2.3	0x108c	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:39.517060041 CEST	8.8.8.8	192.168.2.3	0xec2f	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:43.593290091 CEST	8.8.8.8	192.168.2.3	0x10c3	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:43.623313904 CEST	8.8.4.4	192.168.2.3	0x8a08	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:43.688761950 CEST	8.8.8.8	192.168.2.3	0x3f28	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:47.767203093 CEST	8.8.8.8	192.168.2.3	0xbb44	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:47.799412012 CEST	8.8.4.4	192.168.2.3	0x36de	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:47.833585024 CEST	8.8.8.8	192.168.2.3	0x4651	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:51.921591997 CEST	8.8.8.8	192.168.2.3	0x1e9c	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:51.991132021 CEST	8.8.4.4	192.168.2.3	0x2ee5	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:52.025352955 CEST	8.8.8.8	192.168.2.3	0xf023	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:56.101121902 CEST	8.8.8.8	192.168.2.3	0x8915	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:56.131701946 CEST	8.8.4.4	192.168.2.3	0xa297	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:10:56.173104048 CEST	8.8.8.8	192.168.2.3	0x1bbf	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:00.412239075 CEST	8.8.8.8	192.168.2.3	0x7fb6	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:00.441149950 CEST	8.8.4.4	192.168.2.3	0xdbfb	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2021 23:11:00.476136923 CEST	8.8.8.8	192.168.2.3	0x52c7	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:04.550043106 CEST	8.8.8.8	192.168.2.3	0xda29	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:04.612981081 CEST	8.8.4.4	192.168.2.3	0xf82d	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:04.648161888 CEST	8.8.8.8	192.168.2.3	0xc664	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:08.704226017 CEST	8.8.8.8	192.168.2.3	0xfa5d	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:08.731278896 CEST	8.8.4.4	192.168.2.3	0x4447	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:08.759412050 CEST	8.8.8.8	192.168.2.3	0xb0e8	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:12.802583933 CEST	8.8.8.8	192.168.2.3	0x41ac	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:12.833148956 CEST	8.8.4.4	192.168.2.3	0xb4e5	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)
Jul 21, 2021 23:11:12.866863966 CEST	8.8.8.8	192.168.2.3	0x8f5e	Name error (3)	domingos-50227.portmap.io	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: TRwrC.exe PID: 2044 Parent PID: 5528

General

Start time:	23:09:00
Start date:	21/07/2021
Path:	C:\Users\user\Desktop\TRwrC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\TRwrC.exe'
Imagebase:	0x460000
File size:	207360 bytes
MD5 hash:	EAA9755979D4EDEAC9C48FFB1F42551C
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: 00000000.00000000.205379855.0000000000462000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.205379855.0000000000462000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.205379855.0000000000462000.00000002.00020000.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: 5876 Parent PID: 3388

General

Start time:	23:09:13
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:	0xd20000
File size:	207360 bytes
MD5 hash:	EAA9755979D4EDEAC9C48FFB1F42551C
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: 00000005.00000000.233225156.0000000000D22000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.233225156.0000000000D22000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.233225156.0000000000D22000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.248661530.0000000000D22000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.248661530.0000000000D22000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.248661530.0000000000D22000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.250072753.00000000034D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.250072753.00000000034D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.250132259.00000000044D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.250132259.00000000044D1000.00000004.00000001.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
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis