ID: 452096
Sample Name:
WrNhr6yUD8.exe
Cookbook: default.jbs
Time: 20:25:39
Date: 21/07/2021
Version: 33.0.0 White Diamond

Table of Contents

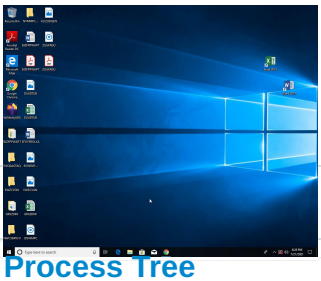
Windows Analysis Report WrNhr6yUD8.exe

Overview

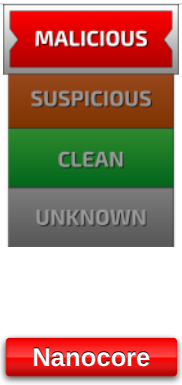
General Information

Sample Name:	WrNhr6yUD8.exe
Analysis ID:	452096
MD5:	fb64fc2471a4892..
SHA1:	334f95083ee83d2.
SHA256:	cc536d630284e6..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

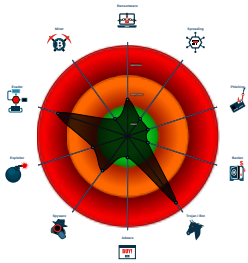


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- 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…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- WrNhr6yUD8.exe (PID: 896 cmdline: 'C:\Users\user\Desktop\WrNhr6yUD8.exe' MD5: FB64FC2471A48928B7989F7E959DE261)
  - WrNhr6yUD8.exe (PID: 5916 cmdline: C:\Users\user\AppData\Local\Temp\WrNhr6yUD8.exe MD5: FB64FC2471A48928B7989F7E959DE261)
- dhcpmon.exe (PID: 5660 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: FB64FC2471A48928B7989F7E959DE261)
  - dhcpmon.exe (PID: 612 cmdline: C:\Users\user\AppData\Local\Temp\dhcpmon.exe MD5: FB64FC2471A48928B7989F7E959DE261)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.507240741.00000000074D0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b0b:$x1: NanoCore.ClientPluginHost • 0x5b44:$x2: IClientNetworkHost
0000000E.00000002.507240741.00000000074D0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5b0b:$x2: NanoCore.ClientPluginHost • 0x5c0f:$s4: PipeCreated • 0x5b25:$s5: IClientLoggingHost
0000000E.00000002.507076827.000000000748000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x8ba5:$x1: NanoCore.ClientPluginHost • 0x8bd2:$x2: IClientNetworkHost
0000000E.00000002.507076827.000000000748000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x8ba5:$x2: NanoCore.ClientPluginHost • 0x9b74:$s2: FileCommand • 0xe576:$s4: PipeCreated • 0x8bbf:$s5: IClientLoggingHost
0000000E.00000002.507595922.000000000759000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5fee:$x1: NanoCore.ClientPluginHost • 0x602b:$x2: IClientNetworkHost

Click to see the 46 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.WrNhr6yUD8.exe.74d0000.26.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b0b:$x1: NanoCore.ClientPluginHost • 0x5b44:$x2: IClientNetworkHost
14.2.WrNhr6yUD8.exe.74d0000.26.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5b0b:$x2: NanoCore.ClientPluginHost • 0x5c0f:$s4: PipeCreated • 0x5b25:$s5: IClientLoggingHost
14.2.WrNhr6yUD8.exe.44b9930.7.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1f1db:$x1: NanoCore.ClientPluginHost • 0x1f1f5:$x2: IClientNetworkHost
14.2.WrNhr6yUD8.exe.44b9930.7.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1f1db:$x2: NanoCore.ClientPluginHost • 0x22518:$s4: PipeCreated • 0x1f1c8:$s5: IClientLoggingHost
14.2.WrNhr6yUD8.exe.7590000.36.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5fee:$x1: NanoCore.ClientPluginHost • 0x602b:$x2: IClientNetworkHost
Click to see the 154 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:

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)

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

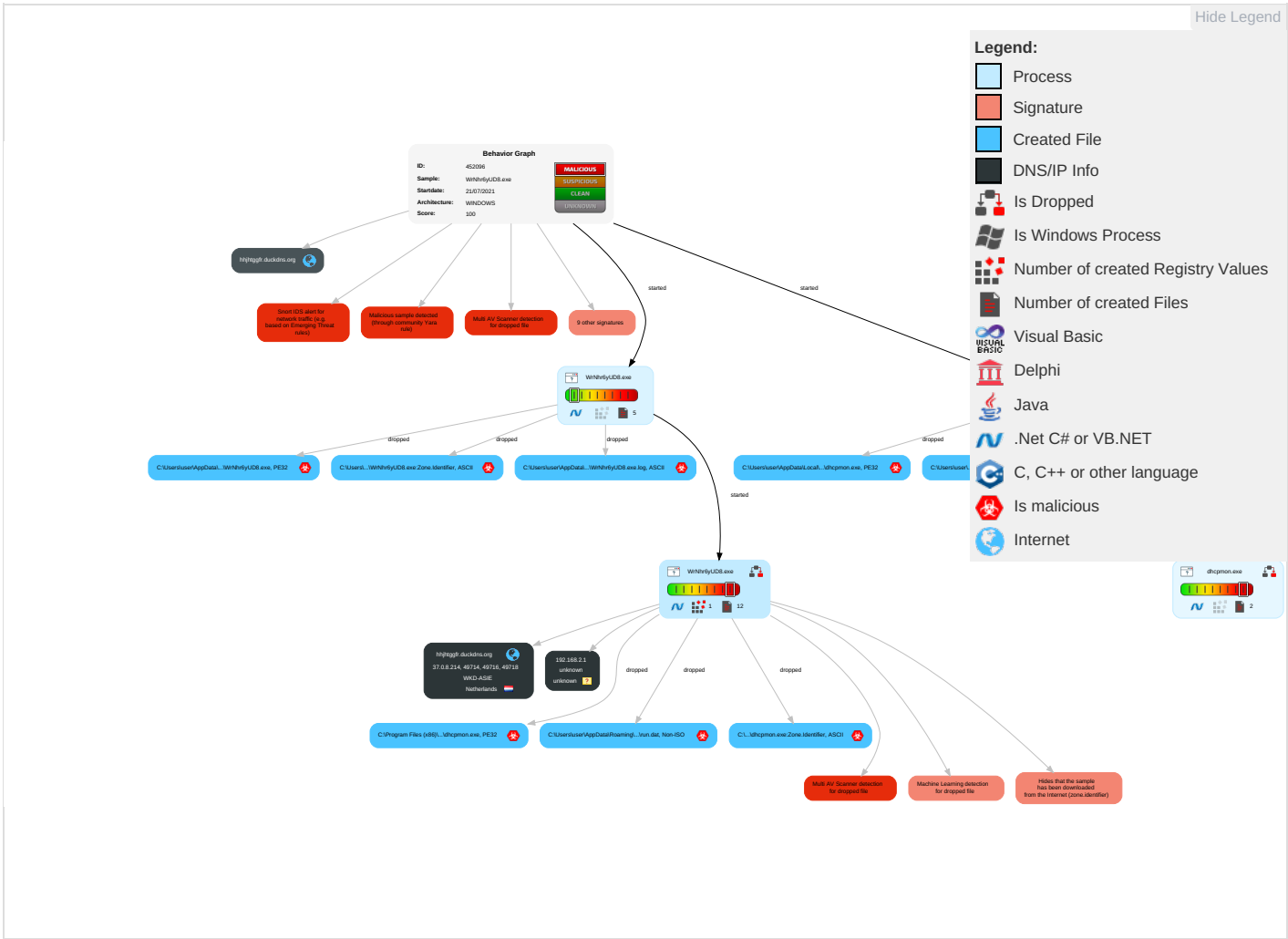
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 2 1 2	Masquerading 2	Input Capture 2 1	Query Registry 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 2	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
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 1 1
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
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

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
WrNhr6yUD8.exe	30%	Virustotal		Browse
WrNhr6yUD8.exe	22%	ReversingLabs	Win32.Trojan.Pwsx	
WrNhr6yUD8.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\WrNhr6yUD8.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	22%	ReversingLabs	Win32.Trojan.Pwsx	
C:\Users\user\AppData\Local\Temp\WrNhr6yUD8.exe	22%	ReversingLabs	Win32.Trojan.Pwsx	
C:\Users\user\AppData\Local\Temp\dhcpmon.exe	22%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.WrNhr6yUD8.exe.4518a28.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File
14.2.WrNhr6yUD8.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.2.WrNhr6yUD8.exe.5c70000.20.unpack	100%	Avira	TR/NanoCore.fadte		Download File
22.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comm_	0%	Avira URL Cloud	safe	
http://www.tiro.com:	0%	Virustotal		Browse
http://www.tiro.com:	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comiv	0%	URL Reputation	safe	
http://www.sajatypeworks.comiv	0%	URL Reputation	safe	
http://www.sajatypeworks.comiv	0%	URL Reputation	safe	
http://www.sajatypeworks.comiv	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.comTF	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.carterandcone.comCd	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.carterandcone.comdDkR	0%	Avira URL Cloud	safe	
http://www.fontbureau.comf	0%	URL Reputation	safe	
http://www.fontbureau.comf	0%	URL Reputation	safe	
http://www.fontbureau.comf	0%	URL Reputation	safe	
http://www.founder.com.cn/cn7	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.sajatypeworks.come-d	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comldvo	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hhjhtggfr.duckdns.org	37.0.8.214	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.0.8.214	hhjhtggfr.duckdns.org	Netherlands		198301	WKD-ASIE	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452096
Start date:	21.07.2021
Start time:	20:25:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	WrNhr6yUD8.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:	26
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@6/12@14/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 60% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 98% • 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
20:27:10	API Interceptor	727x Sleep call for process: WrNhr6yUD8.exe modified
20:27:12	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\AppData\Local\Temp\WrNhr6yUD8.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	888320
Entropy (8bit):	7.140749794967654
Encrypted:	false
SSDEEP:	24576:6ULRbkn8PjhH42j74d8BAk1t1L+PRUyplVnv:6atkAY2YapQUypbn
MD5:	FB64FC2471A48928B7989F7E959DE261
SHA1:	334F95083EE83D20255B87E0BFD4AAE86A922D20
SHA-256:	CC536D630284E622821D1034FADEC488CB35DC72BDFB75EDBD184A638D052F98
SHA-512:	C96A7EF0E0691096E7CD8C841696A4BE951F4B1621C4AA89B39D98E24E9310464558C66EBA3F67600E169DA46D9936D670A26802B2F5550A4804552EF9FC7916
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 22%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....j.... .....@.. ....@.....O.....P..... ....H.....text...p.... ....`.rsrc...P.....@..@.reloc..... .....@..B.....L.....H.....&..L.....<@...p.....b.r...p}.....(.....(....*....0..v.....s....s....(....+. ....(.....{.....3...}.....s....s....(....+. .... (.....{.....3..{....o.....{....o....*...0..g.....+Z. b....&....s.....io.....{....(.....o....o....o.....&..(... ....(.....{.....X}.....{.....3.*.....9<.....0..1.....r1..p(!...("......&.r?..p~#...o$.....("... ....*.....*..(....*^(%.....s&...o'...*..

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\AppData\Local\Temp\WrNhr6yUD8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WrNhr6yUD8.exe.log	
Process:	C:\Users\user\Desktop\WrNhr6yUD8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D 8
Malicious:	**true**
Reputation:	unknown
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, PublicKeyT oken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.C onfiguration, 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\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1119

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D 8
Malicious:	false
Reputation:	unknown
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\Temp\WrNhr6yUD8.exe	
Process:	C:\Users\user\Desktop\WrNhr6yUD8.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	888320
Entropy (8bit):	7.140749794967654
Encrypted:	false
SSDEEP:	24576:6ULRbkn8PjhH42j74d8BAk1t1L+PRUyplVnv:6atkAY2YapQUypbn
MD5:	FB64FC2471A48928B7989F7E959DE261
SHA1:	334F95083EE83D20255B87E0BFD4AAE86A922D20
SHA-256:	CC536D630284E622821D1034FADEC488CB35DC72BDFB75EDBD184A638D052F98
SHA-512:	C96A7EF0E0691096E7CD8C841696A4BE951F4B1621C4AA89B39D98E24E9310464558C66EBA3F67600E169DA46D9936D670A26802B2F5550A4804552EF9FC7916
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 22%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....j.... .....@.. ....@.....O.....P..... ....H.....text...p.... ....`.rsrc...P.....@..@.reloc..... .....@..B.....L.....H.....&..L.....<@...p.....b.r...p}.....(.....(....*....0..v.....s....s....(....+. ....(.....{.....3...}.....s....s....(....+. .... (.....{.....3..{....o.....{....o....*...0..g.....+Z. b....&....s.....io.....{....(.....o....o....o.....&..(... ....(.....{.....X}.....{.....3.*.....9<.....0..1.....r1..p(!...("......&.r?..p~#...o$.....("... ....*.....*..(....*^(%.....s&...o'...*..

C:\Users\user\AppData\Local\Temp\WrNhr6yUD8.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\WrNhr6yUD8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp\dhcpmon.exe	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	888320
Entropy (8bit):	7.140749794967654
Encrypted:	false
SSDEEP:	24576:6ULRbkn8PjhH42j74d8BAk1t1L+PRUyplVnv:6atkAY2YapQUypbn
MD5:	FB64FC2471A48928B7989F7E959DE261

C:\Users\user\AppData\Local\Temp\dhcpmon.exe	
SHA1:	334F95083EE83D20255B87E0BFD4AAE86A922D20
SHA-256:	CC536D630284E622821D1034FADEC488CB35DC72BDFB75EDBD184A638D052F98
SHA-512:	C96A7EF0E0691096E7CD8C841696A4BE951F4B1621C4AA89B39D98E24E9310464558C66EBA3F67600E169DA46D9936D670A26802B2F5550A4804552EF9FC7916
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 22%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....j.... .....@.. ....@.....O.....P..... ....H.....text...p.... ....`.rsrc...P.....@..@.reloc..... .....@..B.....L.....H.....&..L.....<@...p.....b.r...p}.....(....(...*....0..v.....s....s....(....+. ....(.....{.....3...}.....s....s....(....+. .... (.....{.....3..{....o.....{....o....*...0..g.....+Z. b....&....s.....io.....{....(....o....o....o.....&..(... ....(.....{.....X}.....{.....3.*.....9<.....0..1.....r1..p(!...("......&.r?..p~#...o$.....("... ....*.....*..(....*^(%.....s&...o'...*..

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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\AppData\Local\Temp\WrNhr6yUD8.exe
File Type:	data
Category:	dropped
Size (bytes):	2088
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCe
MD5:	0D6805D12813A857D50D42D6EE2CCAB0
SHA1:	78D83F009D842F21FE2AB0EAFFD00E5AAD1776F4
SHA-256:	182E0F8AA959549D61C66D049645BA8445D86AEAD2B8C3552A9836FA1E5BD484
SHA-512:	5B29496F3AB3CCB915CF37042F4956BB00E577B5F15457A5A739BE1BD50C481FB7E3297EED575DCA7A7BD30ECBC140DD3666CD7DEDD25DFB7AEB41A1B5BEI A4A
Malicious:	false
Reputation:	unknown
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\WrNhr6yUD8.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:dTzz8:m
MD5:	B78ADC14B1CC69A8126D1F62947CCF3A
SHA1:	D4017FC3B5F7A40FDE16148CCA2902D48FB5D659
SHA-256:	C3527D0EDD6F06CB1EABFD50BA93A43EE03D1273E4CFFD0A7476FC1EF59C239B
SHA-512:	A1880116A392AA5A6BA8AC1F5CEE22AC2AC60268F8EFF83466F594EA92FF773BA6C410C2B5C776B7D5C515321A8DEE7DC74403AE72436F224A20BAB8DB9AA3 28
Malicious:	**true**
Reputation:	unknown

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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\AppData\Local\Temp\WrNhr6yUD8.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\AppData\Local\Temp\WrNhr6yUD8.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
Reputation:	unknown
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v."".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_..&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.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):	7.140749794967654
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	WrNhr6yUD8.exe
File size:	888320
MD5:	fb64fc2471a48928b7989f7e959de261
SHA1:	334f95083ee83d20255b87e0bfd4aae86a922d20
SHA256:	cc536d630284e622821d1034fadec488cb35dc72bdfb75edbd184a638d052f98
SHA512:	c96a7ef0e0691096e7cd8c841696a4be951f4b1621c4aa89b39d98e24e9310464558c66eba3f67600e169da46d9936d670a26802b2f5550a4804552ef9fc7916
SSDEEP:	24576:6ULRbkn8PjhH42j74d8BAk1t1L+PRUyplVnv:6atkAY2YapQUypbn

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....j.... ....@.. .....@.....

File Icon

Icon Hash:	64e4cc8df0f0f0b0

Static PE Info

General

Entrypoint:	0x4cb16a
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:	0xF8B1A194 [Tue Mar 21 13:26:44 2102 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	0xc9170	0xc9200	False	0.785982898928	data	7.02528915193	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xcc000	0xf750	0xf800	False	0.812531502016	data	7.51816910204	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xdc000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/21/21-20:27:13.807230	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49714	8234	192.168.2.5	37.0.8.214
07/21/21-20:27:21.758849	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49716	8234	192.168.2.5	37.0.8.214

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/21/21-20:27:28.036498	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49718	8234	192.168.2.5	37.0.8.214
07/21/21-20:27:35.087761	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	8234	192.168.2.5	37.0.8.214
07/21/21-20:27:43.150923	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	8234	192.168.2.5	37.0.8.214
07/21/21-20:27:49.130581	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	8234	192.168.2.5	37.0.8.214
07/21/21-20:27:54.695591	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49729	8234	192.168.2.5	37.0.8.214
07/21/21-20:28:01.673401	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	8234	192.168.2.5	37.0.8.214
07/21/21-20:28:07.767664	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	8234	192.168.2.5	37.0.8.214
07/21/21-20:28:13.611239	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49734	8234	192.168.2.5	37.0.8.214
07/21/21-20:28:21.114575	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	8234	192.168.2.5	37.0.8.214
07/21/21-20:28:28.020886	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	8234	192.168.2.5	37.0.8.214
07/21/21-20:28:34.420594	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	8234	192.168.2.5	37.0.8.214
07/21/21-20:28:40.378034	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	8234	192.168.2.5	37.0.8.214

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2021 20:27:12.864238024 CEST	192.168.2.5	8.8.8.8	0x7c8e	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 20:27:21.396034956 CEST	192.168.2.5	8.8.8.8	0x9c2d	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 20:27:27.831329107 CEST	192.168.2.5	8.8.8.8	0x2c79	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 20:27:34.900463104 CEST	192.168.2.5	8.8.8.8	0x51fa	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 20:27:43.028851032 CEST	192.168.2.5	8.8.8.8	0xaf47	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 20:27:49.074486017 CEST	192.168.2.5	8.8.8.8	0x1510	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 20:27:54.649091959 CEST	192.168.2.5	8.8.8.8	0x9572	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 20:28:01.630784988 CEST	192.168.2.5	8.8.8.8	0x8c91	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 20:28:07.725210905 CEST	192.168.2.5	8.8.8.8	0x8334	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 20:28:12.748063087 CEST	192.168.2.5	8.8.8.8	0x7148	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 20:28:21.065098047 CEST	192.168.2.5	8.8.8.8	0x71e3	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 20:28:27.930370092 CEST	192.168.2.5	8.8.8.8	0x47de	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 20:28:34.372925997 CEST	192.168.2.5	8.8.8.8	0xb3b1	Standard query (0)	hhjhtggfr.duckdns.org	A (IP address)	IN (0x0001)
Jul 21, 2021 20:28:40.335563898 CEST	192.168.2.5	8.8.8.8	0xf1ea	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
Jul 21, 2021 20:27:12.988148928 CEST	8.8.8.8	192.168.2.5	0x7c8e	No error (0)	hhjhtggfr.duckdns.org		37.0.8.214	A (IP address)	IN (0x0001)
Jul 21, 2021 20:27:21.521564960 CEST	8.8.8.8	192.168.2.5	0x9c2d	No error (0)	hhjhtggfr.duckdns.org		37.0.8.214	A (IP address)	IN (0x0001)
Jul 21, 2021 20:27:27.959212065 CEST	8.8.8.8	192.168.2.5	0x2c79	No error (0)	hhjhtggfr.duckdns.org		37.0.8.214	A (IP address)	IN (0x0001)
Jul 21, 2021 20:27:35.025049925 CEST	8.8.8.8	192.168.2.5	0x51fa	No error (0)	hhjhtggfr.duckdns.org		37.0.8.214	A (IP address)	IN (0x0001)
Jul 21, 2021 20:27:43.043302059 CEST	8.8.8.8	192.168.2.5	0xaf47	No error (0)	hhjhtggfr.duckdns.org		37.0.8.214	A (IP address)	IN (0x0001)
Jul 21, 2021 20:27:49.087997913 CEST	8.8.8.8	192.168.2.5	0x1510	No error (0)	hhjhtggfr.duckdns.org		37.0.8.214	A (IP address)	IN (0x0001)
Jul 21, 2021 20:27:54.661930084 CEST	8.8.8.8	192.168.2.5	0x9572	No error (0)	hhjhtggfr.duckdns.org		37.0.8.214	A (IP address)	IN (0x0001)
Jul 21, 2021 20:28:01.644711971 CEST	8.8.8.8	192.168.2.5	0x8c91	No error (0)	hhjhtggfr.duckdns.org		37.0.8.214	A (IP address)	IN (0x0001)
Jul 21, 2021 20:28:07.739787102 CEST	8.8.8.8	192.168.2.5	0x8334	No error (0)	hhjhtggfr.duckdns.org		37.0.8.214	A (IP address)	IN (0x0001)
Jul 21, 2021 20:28:12.873614073 CEST	8.8.8.8	192.168.2.5	0x7148	No error (0)	hhjhtggfr.duckdns.org		37.0.8.214	A (IP address)	IN (0x0001)
Jul 21, 2021 20:28:21.081299067 CEST	8.8.8.8	192.168.2.5	0x71e3	No error (0)	hhjhtggfr.duckdns.org		37.0.8.214	A (IP address)	IN (0x0001)
Jul 21, 2021 20:28:27.946304083 CEST	8.8.8.8	192.168.2.5	0x47de	No error (0)	hhjhtggfr.duckdns.org		37.0.8.214	A (IP address)	IN (0x0001)
Jul 21, 2021 20:28:34.385742903 CEST	8.8.8.8	192.168.2.5	0xb3b1	No error (0)	hhjhtggfr.duckdns.org		37.0.8.214	A (IP address)	IN (0x0001)
Jul 21, 2021 20:28:40.350263119 CEST	8.8.8.8	192.168.2.5	0xf1ea	No error (0)	hhjhtggfr.duckdns.org		37.0.8.214	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WrNhr6yUD8.exe PID: 896 Parent PID: 5644

General

Start time:	20:26:31
Start date:	21/07/2021
Path:	C:\Users\user\Desktop\WrNhr6yUD8.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\WrNhr6yUD8.exe'
Imagebase:	0x320000
File size:	888320 bytes
MD5 hash:	FB64FC2471A48928B7989F7E959DE261
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: 00000000.00000002.308987203.00000000038F6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.308987203.00000000038F6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.308987203.00000000038F6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.308863362.0000000003857000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.308863362.0000000003857000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.308863362.0000000003857000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.308575708.00000000028DA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.308575708.00000000028DA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: WrNhr6yUD8.exe PID: 5916 Parent PID: 896

General

Start time:	20:27:06
Start date:	21/07/2021
Path:	C:\Users\user\AppData\Local\Temp\WrNhr6yUD8.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\WrNhr6yUD8.exe
Imagebase:	0xfa0000
File size:	888320 bytes
MD5 hash:	FB64FC2471A48928B7989F7E959DE261
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: 0000000E.00000002.507240741.00000000074D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.507240741.00000000074D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.507076827.0000000007480000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.507076827.0000000007480000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.507595922.0000000007590000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.507595922.0000000007590000.00000004.00000001.sdmp, Author:

	Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.507410107.0000000007510000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.507410107.0000000007510000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.504364191.0000000004501000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.507284046.00000000074E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.507284046.00000000074E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.496594455.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.496594455.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.496594455.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.507147677.00000000074B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.507147677.00000000074B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.504446438.0000000004581000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.504446438.0000000004581000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.505956339.0000000005A20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.505956339.0000000005A20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.504700403.000000000479F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.507370869.0000000007500000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.507370869.0000000007500000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.500382926.00000000034B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.500382926.00000000034B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.507319723.00000000074F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.507319723.00000000074F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.506071191.0000000005C70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.506071191.0000000005C70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.506071191.0000000005C70000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.507514929.0000000007550000.00000004.00000001.sdmp, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 22%, ReversingLabs
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: 5660 Parent PID: 3472

General

Start time:	20:27:21
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:	0x810000
File size:	888320 bytes
MD5 hash:	FB64FC2471A48928B7989F7E959DE261
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: 00000010.00000002.409979115.0000000002E9D000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.409979115.0000000002E9D000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.410463215.0000000003E98000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.410463215.0000000003E98000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.410463215.0000000003E98000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 22%, ReversingLabs
Reputation:	low

File Activities — Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 612 Parent PID: 5660

General

Start time:	20:27:52
Start date:	21/07/2021
Path:	C:\Users\user\AppData\Local\Temp\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\dhcpmon.exe
Imagebase:	0xc80000
File size:	888320 bytes
MD5 hash:	FB64FC2471A48928B7989F7E959DE261

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: 00000016.00000002.424925007.00000000040E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.424925007.00000000040E9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.424776175.00000000030E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.424776175.00000000030E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.422787857.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.422787857.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.422787857.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 22%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis