ID: 356809
Sample Name:
UCDR562uYv.exe
Cookbook: default.jbs
Time: 17:06:23
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright null 2021

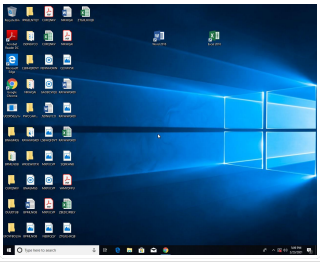
Analysis Report UCDR562uYv.exe

Overview

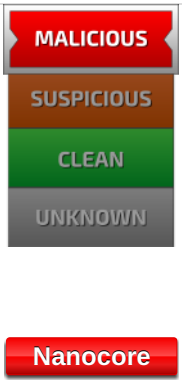
General Information

Sample Name:	UCDR562uYv.exe
Analysis ID:	356809
MD5:	cf3cbcf8eed33d5...
SHA1:	f64c016fdea3bbd..
SHA256:	b9ebcdd39a9e00..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



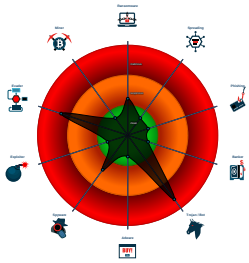
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Binary contains a suspicious time st…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…
- Uses dynamic DNS services

Classification



Startup

- **System is w10x64**
- UCDR562uYv.exe (PID: 6804 cmdline: 'C:\Users\user\Desktop\UCDR562uYv.exe' MD5: CF3CBCF8EED33D5DD9778C4914B21FD9)
  - schtasks.exe (PID: 7000 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lRvvjxua' /XML 'C:\Users\user\AppData\Local\Temp\tmp483E.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7024 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - UCDR562uYv.exe (PID: 7060 cmdline: {path} MD5: CF3CBCF8EED33D5DD9778C4914B21FD9)
- dhcpmon.exe (PID: 4964 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: CF3CBCF8EED33D5DD9778C4914B21FD9)
  - schtasks.exe (PID: 6364 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lRvvjxua' /XML 'C:\Users\user\AppData\Local\Temp\tmp86BE.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6352 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 6440 cmdline: {path} MD5: CF3CBCF8EED33D5DD9778C4914B21FD9)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "2e8224ea-0d1f-4740-8aea-f16b1e97c433",
  "Group": "GODSPOWER",
  "Domain1": "kene3210.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 3210,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.384846526.000000006456000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1c79f5:$x1: NanoCore.ClientPluginHost • 0x1c7a32:$x2: IClientNetworkHost • 0x1cb565:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000008.00000002.384846526.000000006456000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000008.00000002.384846526.000000006456000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1c775d:$a: NanoCore • 0x1c776d:$a: NanoCore • 0x1c79a1:$a: NanoCore • 0x1c79b5:$a: NanoCore • 0x1c79f5:$a: NanoCore • 0x1c77bc:$b: ClientPlugin • 0x1c79be:$b: ClientPlugin • 0x1c79fe:$b: ClientPlugin • 0x14ee18:$c: ProjectData • 0x1c78e3:$c: ProjectData • 0x14fb74:$d: DESCrypto • 0x1c82ea:$d: DESCrypto • 0x1cfcb6:$e: KeepAlive • 0x1cdca4:$g: LogClientMessage • 0x1c9e9f:$i: get_Connected • 0x1c8620:$j: #=q • 0x1c8650:$j: #=q • 0x1c866c:$j: #=q • 0x1c869c:$j: #=q • 0x1c86b8:$j: #=q • 0x1c86d4:$j: #=q
00000005.00000002.599662311.000000003181000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000005.00000002.604263829.00000000062B0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost

Click to see the 31 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.UCDR562uYv.exe.41cff6c.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0x28271:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost • 0x2829e:$x2: IClientNetworkHost

Copyright null 2021

Source	Rule	Description	Author	Strings
5.2.UCDR562uYv.exe.41cff6c.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x28271:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0x2934c:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost • 0x2828b:$s5: IClientLoggingHost
5.2.UCDR562uYv.exe.41cff6c.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
5.2.UCDR562uYv.exe.41d4595.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x23c48:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x23c75:$x2: IClientNetworkHost
5.2.UCDR562uYv.exe.41d4595.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0x23c48:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0x24d23:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost • 0x23c62:$s5: IClientLoggingHost
Click to see the 66 entries				

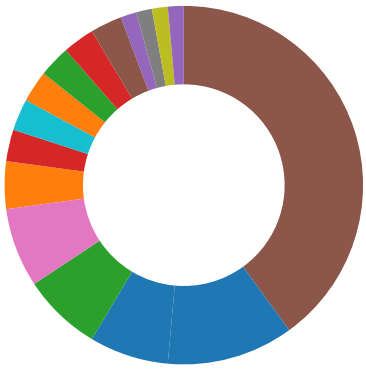
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Binary contains a suspicious time stamp

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

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)

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

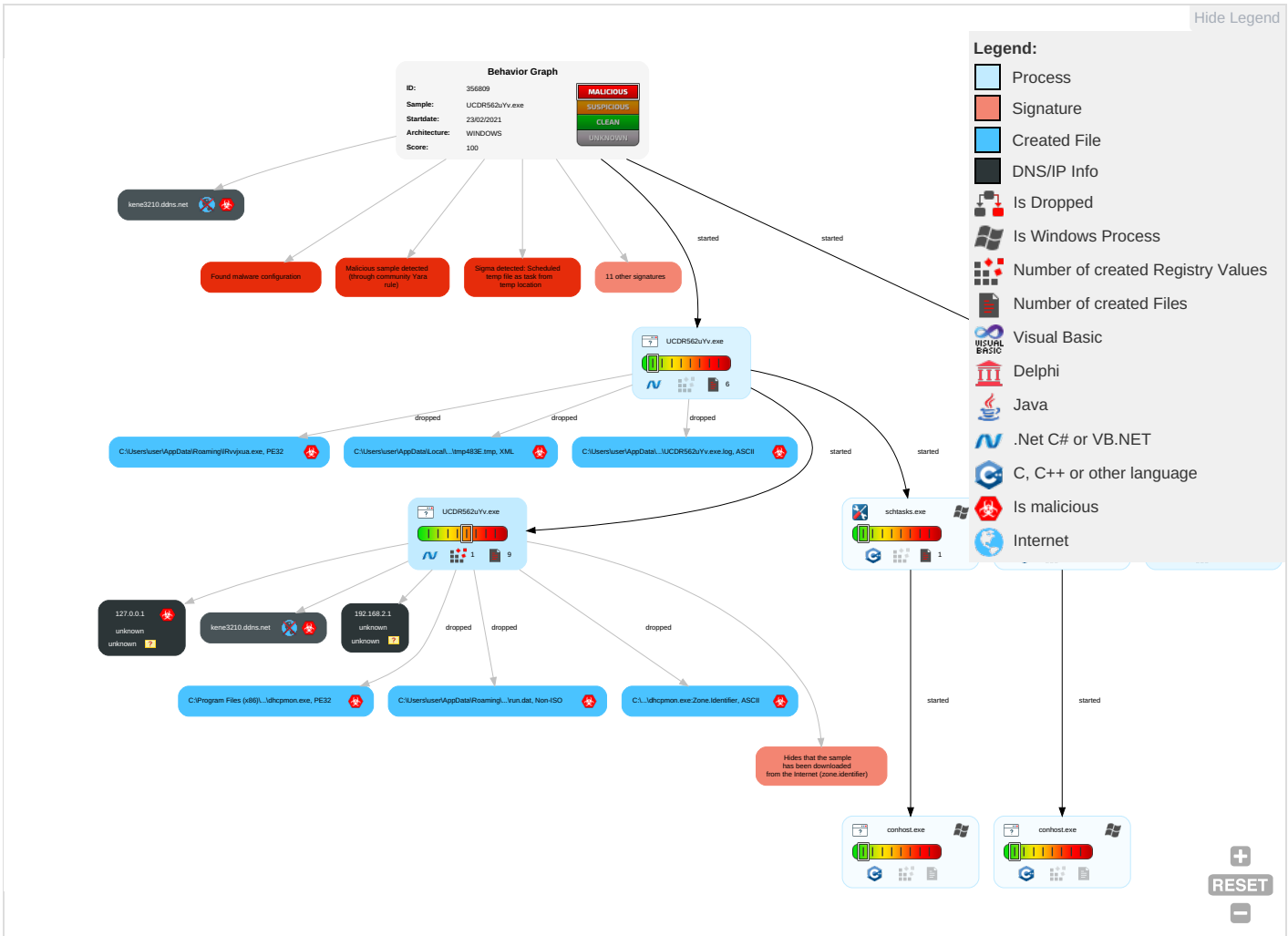
Yara detected Nanocore RAT

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	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 2	Masquerading 2	Input Capture 2 1	Security Software Discovery 1 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdro Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Remote Access Software 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit S Track De Location

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 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	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P
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	Downgra Insecure Protocols
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	Rogue C Base Sta

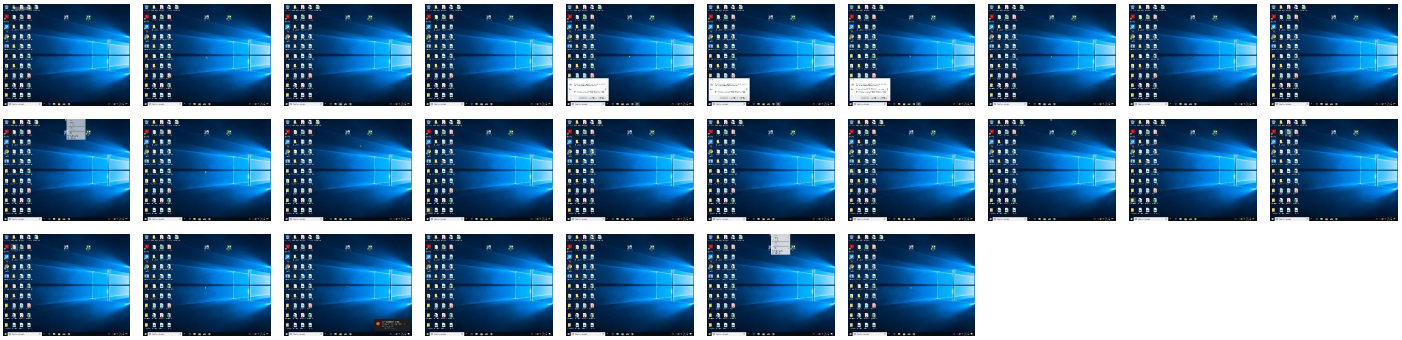
Behavior Graph



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
UCDR562uYv.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\lRvvjxua.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.UCDR562uYv.exe.62b0000.11.unpack	100%	Avira	TR/NanoCore.fadte		Download File
5.2.UCDR562uYv.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
kene3210.ddns.net	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kene3210.ddns.net	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
kene3210.ddns.net	true	• Avira URL Cloud: safe	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	UCDR562uYv.exe, 00000000.00000002.344576426.0000000002F51000.00000004.00000001.sdmp, dhcpmon.exe, 00000008.00000002.382464682.00000000032A1000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356809
Start date:	23.02.2021
Start time:	17:06:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	UCDR562uYv.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:	28
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

Copyright null 2021

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@12/8@45/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 13.64.90.137, 40.88.32.150, 23.211.6.115, 104.42.151.234, 168.61.161.212, 52.147.198.201, 104.43.193.48, 13.88.21.125, 51.11.168.160, 2.20.142.209, 2.20.142.210, 51.103.5.159, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194, 184.30.24.56, 51.104.139.180 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:07:16	API Interceptor	1005x Sleep call for process: UCDR562uYv.exe modified
17:07:22	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
17:07:33	API Interceptor	33x Sleep call for process: dhcpmon.exe modified

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\UCDR562uYv.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	820224
Entropy (8bit):	7.935160892507609
Encrypted:	false
SSDEEP:	12288:czXzZns2m0eCQQeD69UZLvxCyqmexnN2dMIrCREQlq0+115aH2la60LHHjMR:czXzlZTQ1W9UZNCLxNumRbq0sKS
MD5:	CF3CBCF8EED33D5DD9778C4914B21FD9
SHA1:	F64C016FDEA3BBD98964BDFC2FDA33D7AABA1361
SHA-256:	B9EBCDD39A9E00E766DAFBF2EA752B7310D179F65B0D989C402CF45CF3EFC321
SHA-512:	FF4FB2D3A349BCAC2027AC92D18FF44DD3CF46BDD128C4F6FB0FC86EE6A36FE7CFFE61159E4C53EFDC2104785C0CBDE68BA4D34E1DAB55E6F2F54C4B3B83C9F6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....I.....0..z..... .....@.. ....@.....O..... ....H.....text... x... ...z..... ..`.rsrc.....\|.....@..@.reloc..... .....@..B.....H.....>...".....Q....`...6.....0..H.....(.....".....".....sU...}.....".....sU...}.....}.....~....k}....*.0..}.....{.....,#...{.....{....(W...}.....(.....+N..~....k}.....o;...oK...o[....o;...oK...o]..."...?~/...kZY~....kY.sU...}.....*....0..I.....(....s.....{....o[...~....kY.{....o]...~....kY.~....Zk.~....Zko.....*....0.....{....o[...~..kX"..pAX~$...k....,...{...".....{....o[...Zo\.....{....o[...~....

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

Process:	C:\Users\user\Desktop\UCDR562uYv.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\UCDR562uYv.exe.log	
Process:	C:\Users\user\Desktop\UCDR562uYv.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4VE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz5
MD5:	6C42AAF2F2FABAD2BAB70543AE48CEDB
SHA1:	8552031F83C078FE1C035191A32BA43261A63DA9
SHA-256:	51D07DD061EA9665DA070B95A4AC2AC17E20524E30BF6A0DA8381C2AF29CA967
SHA-512:	014E89857B811765EA7AA0B030AB04A2DA1957571608C4512EC7662F6A4DCE8B0409626624DABC96CBFF079E7F0F4A916E6F49C789E00B6E46AD37C36C806DC
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4VE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz5
MD5:	6C42AAF2F2FABAD2BAB70543AE48CEDB
SHA1:	8552031F83C078FE1C035191A32BA43261A63DA9
SHA-256:	51D07DD061EA9665DA070B95A4AC2AC17E20524E30BF6A0DA8381C2AF29CA967
SHA-512:	014E89857B811765EA7AA0B030AB04A2DA1957571608C4512EC7662F6A4DCE8B0409626624DABC96CBFF079E7F0F4A916E6F49C789E00B6E46AD37C36C806DC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp483E.tmp	
Process:	C:\Users\user\Desktop\UCDR562uYv.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1653
Entropy (8bit):	5.1561818136292406
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3Dtn:cbha7JlNQV/rydbz9I3YODOLNdq3n
MD5:	FCBA3D1338C2D43D4E72F9CBAF773762
SHA1:	B6BC93238A70C344414AB57444036D709C01D60F
SHA-256:	DB223B21CB6D8D57F5AB1D29B7723287D5F7C8C18DE6F1AADF370C7139C3A181
SHA-512:	C2F608DFB37D0221B2E4B8A801248034E65B2B453680199B1BD88A57DDDA61FAE7148C6DA2E4C89A2FE511AC81D312A8BAC3F7896C09D486592E9DC76BE059

C:\Users\user\AppData\Local\Temp\tmp483E.tmp

Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmp86BE.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1653
Entropy (8bit):	5.1561818136292406
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3Dtn:cbha7JlNQV/rydbz9I3YODOLNdq3n
MD5:	FCBA3D1338C2D43D4E72F9CBAF773762
SHA1:	B6BC93238A70C344414AB57444036D709C01D60F
SHA-256:	DB223B21CB6D8D57F5AB1D29B7723287D5F7C8C18DE6F1AADF370C7139C3A181
SHA-512:	C2F608DFB37D0221B2E4B8A801248034E65B2B453680199B1BD88A57DDDA61FAE7148C6DA2E4C89A2FE511AC81D312A8BAC3F7896C09D486592E9DC76BE059 2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

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

Process:	C:\Users\user\Desktop\UCDR562uYv.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:I:I
MD5:	FE414FB2AECE1D020A3088145D7022DF
SHA1:	0F5B246B3615A1D85AAFAE3B177E7051CB8500E3
SHA-256:	80699AA482EC36FAF3CA7DEC15E7FC1903A333C8B84E4543E05CC304DA52BB94
SHA-512:	C44E60FE8A1B912771D040DA430954FD13CB2905C46CFF00B4337D87E11473B1E8FEAB0ADB805F7566B859385411E473594A28C326EEA2F4D583C29F2D60DDC
Malicious:	**true**
Preview:	FAV.`..H

C:\Users\user\AppData\Roaming\IRvvjxua.exe

Process:	C:\Users\user\Desktop\UCDR562uYv.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	820224
Entropy (8bit):	7.935160892507609
Encrypted:	false
SSDEEP:	12288:czXzZns2m0eCQQeD69UZLvxCyqmexnN2dMIrCREQlq0+115aH2la60LHHjMR:czXzlZTQ1W9UZNCLxNumRbq0sKS
MD5:	CF3CBCF8EED33D5DD9778C4914B21FD9
SHA1:	F64C016FDEA3BBD98964BDFC2FDA33D7AABA1361
SHA-256:	B9EBCDD39A9E00E766DAFBF2EA752B7310D179F65B0D989C402CF45CF3EFC321
SHA-512:	FF4FB2D3A349BCAC2027AC92D18FF44DD3CF46BDD128C4F6FB0FC86EE6A36FE7CFFE61159E4C53EFDC2104785C0CBDE68BA4D34E1DAB55E6F2F54C4B3B83 C9F6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

C:\Users\user\AppData\Roaming\lRvvjxua.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....l.....0..z..... .....@.. ....@.....O..... ....H.....text... x... ...z..... ..`.rsrc.....\|.....@..@.reloc..... .....@..B.....H.....>..."....Q....`...6.....0..H.....(....."...."....sU...}....."...."....sU...}.....}.....~....k}....*.0..}.....{.....,#...{.....{.... (W...}.....(.....+N..~....k}.....o;...oK...o[....o;...oK...o]..."...?~/...kZY~....kY.sU...}....*....0..l.....(....s.....{....o[...~....kY.{....o]...~....kY.~....Zk.~....Zko....*....0.....{....o[...~.. ..kX"..pAX~$...k....,...{...."....{....o[...Zo\.....{....o[...~....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.935160892507609
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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	UCDR562uYv.exe
File size:	820224
MD5:	cf3cbcf8eed33d5dd9778c4914b21fd9
SHA1:	f64c016fdea3bbd98964bdfc2fda33d7aaba1361
SHA256:	b9ebcdd39a9e00e766dafbf2ea752b7310d179f65b0d989c402cf45cf3efc321
SHA512:	ff4fb2d3a349bcac2027ac92d18ff44dd3cf46bdd128c4f6fb0fc86ee6a36fe7cffe61159e4c53efdc2104785c0cbde68ba4d34e1dab55e6f2f54c4b3b83c9f6
SSDEEP:	12288:czXzZns2m0eCQQeD69UZLvxCyqmexnN2dMIrCREQlq0+115aH2la60LHHjMR:czXzlZTQ1W9UZNCLxNumRbq0sKS
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....l.....0..z..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c981a
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:	0xEE6CE2B9 [Wed Oct 3 14:35:37 2096 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc97c8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xca000	0x594	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xcc000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xc97ac	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xc7820	0xc7a00	False	0.948410349483	data	7.9374544928	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xca000	0x594	0x600	False	0.416666666667	data	4.05140003811	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xcc000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Copyright null 2021

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xca090	0x304	data		
RT_MANIFEST	0xca3a4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019
Assembly Version	1.0.0.0
InternalName	.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	PongGame
ProductVersion	1.0.0.0
FileDescription	PongGame
OriginalFilename	.exe

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:07:05.536439896 CET	58377	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:05.587552071 CET	53	58377	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:07.290556908 CET	55074	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:07.339354038 CET	53	55074	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:08.457015991 CET	54513	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:08.505650997 CET	53	54513	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:08.712867975 CET	62044	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:08.774600029 CET	53	62044	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:09.437637091 CET	63791	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:09.489430904 CET	53	63791	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:10.362874985 CET	64267	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:10.411917925 CET	53	64267	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:11.565485954 CET	49448	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:11.619564056 CET	53	49448	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:13.612128019 CET	60342	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:13.663732052 CET	53	60342	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:14.628809929 CET	61346	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:14.679582119 CET	53	61346	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:15.816450119 CET	51774	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:15.865339041 CET	53	51774	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:18.441236019 CET	56023	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:18.491549015 CET	53	56023	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:19.496987104 CET	58384	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:19.557121038 CET	53	58384	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:21.749881983 CET	60261	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:21.801907063 CET	53	60261	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:22.733513117 CET	56061	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:22.782121897 CET	53	56061	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:24.091799021 CET	58336	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:07:24.143296957 CET	53	58336	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:24.744170904 CET	53781	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:24.809181929 CET	53	53781	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:24.857589960 CET	54064	53	192.168.2.6	8.8.4.4
Feb 23, 2021 17:07:24.921189070 CET	53	54064	8.8.4.4	192.168.2.6
Feb 23, 2021 17:07:25.070523024 CET	52811	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:25.199552059 CET	53	52811	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:29.333532095 CET	55299	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:29.393665075 CET	53	55299	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:29.421070099 CET	63745	53	192.168.2.6	8.8.4.4
Feb 23, 2021 17:07:29.481549025 CET	53	63745	8.8.4.4	192.168.2.6
Feb 23, 2021 17:07:29.498599052 CET	50055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:29.550241947 CET	53	50055	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:31.474987984 CET	61374	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:31.527160883 CET	53	61374	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:33.832477093 CET	50339	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:33.893160105 CET	53	50339	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:33.941015005 CET	63307	53	192.168.2.6	8.8.4.4
Feb 23, 2021 17:07:33.998241901 CET	53	63307	8.8.4.4	192.168.2.6
Feb 23, 2021 17:07:34.048948050 CET	49694	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:34.112076998 CET	54982	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:34.112571955 CET	53	49694	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:34.163244009 CET	53	54982	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:35.108508110 CET	50010	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:35.157372952 CET	53	50010	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:36.159936905 CET	63718	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:36.210747957 CET	53	63718	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:37.036612034 CET	62116	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:37.086174965 CET	53	62116	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:42.994801044 CET	63816	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:43.044852018 CET	53	63816	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:53.348172903 CET	55014	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:53.410068989 CET	53	55014	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:53.441025019 CET	62208	53	192.168.2.6	8.8.4.4
Feb 23, 2021 17:07:53.489680052 CET	53	62208	8.8.4.4	192.168.2.6
Feb 23, 2021 17:07:53.530246973 CET	57574	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:53.582711935 CET	53	57574	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:57.711498976 CET	51818	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:57.773730993 CET	53	51818	8.8.8.8	192.168.2.6
Feb 23, 2021 17:07:57.802349091 CET	56628	53	192.168.2.6	8.8.4.4
Feb 23, 2021 17:07:57.853434086 CET	53	56628	8.8.4.4	192.168.2.6
Feb 23, 2021 17:07:57.914513111 CET	60778	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:07:57.973037004 CET	53	60778	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:00.737786055 CET	53799	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:00.795958042 CET	53	53799	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:02.050817013 CET	54683	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:02.110687017 CET	53	54683	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:02.114079952 CET	59329	53	192.168.2.6	8.8.4.4
Feb 23, 2021 17:08:02.172787905 CET	53	59329	8.8.4.4	192.168.2.6
Feb 23, 2021 17:08:02.210747957 CET	64021	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:02.268100977 CET	53	64021	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:02.327007055 CET	56129	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:02.378273010 CET	53	56129	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:05.620502949 CET	58177	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:05.696355104 CET	53	58177	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:06.283384085 CET	50700	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:06.340379953 CET	53	50700	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:07.008158922 CET	54069	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:07.123744011 CET	53	54069	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:07.620605946 CET	61178	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:07.680356026 CET	53	61178	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:08.533556938 CET	57017	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:08.594821930 CET	53	57017	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:09.640419960 CET	56327	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:08:09.689125061 CET	53	56327	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:09.958806038 CET	50243	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:10.033878088 CET	53	50243	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:11.465976954 CET	62055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:11.527086020 CET	53	62055	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:12.865911007 CET	61249	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:12.916166067 CET	53	61249	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:13.867964983 CET	65252	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:13.918304920 CET	53	65252	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:14.662750006 CET	64367	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:14.720032930 CET	53	64367	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:17.284904957 CET	55066	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:17.347429037 CET	53	55066	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:21.794615984 CET	60211	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:21.844912052 CET	53	60211	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:21.848858118 CET	56570	53	192.168.2.6	8.8.4.4
Feb 23, 2021 17:08:21.899621010 CET	53	56570	8.8.4.4	192.168.2.6
Feb 23, 2021 17:08:22.043221951 CET	58454	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:22.100816965 CET	53	58454	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:26.147032976 CET	55180	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:26.204144955 CET	53	55180	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:26.210582018 CET	58721	53	192.168.2.6	8.8.4.4
Feb 23, 2021 17:08:26.262346029 CET	53	58721	8.8.4.4	192.168.2.6
Feb 23, 2021 17:08:26.447410107 CET	57691	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:26.512365103 CET	53	57691	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:30.565412045 CET	52943	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:30.624352932 CET	53	52943	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:30.700958967 CET	59489	53	192.168.2.6	8.8.4.4
Feb 23, 2021 17:08:30.752542973 CET	53	59489	8.8.4.4	192.168.2.6
Feb 23, 2021 17:08:30.804845095 CET	64022	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:30.861898899 CET	53	64022	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:44.132929087 CET	60023	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:44.191557884 CET	53	60023	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:49.882972002 CET	57193	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:49.934500933 CET	53	57193	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:50.045794964 CET	50248	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:50.100102901 CET	53	50248	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:50.103560925 CET	64413	53	192.168.2.6	8.8.4.4
Feb 23, 2021 17:08:50.153879881 CET	53	64413	8.8.4.4	192.168.2.6
Feb 23, 2021 17:08:50.245938063 CET	60429	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:50.308901072 CET	53	60429	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:52.084875107 CET	60345	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:52.140256882 CET	53	60345	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:54.377499104 CET	58730	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:54.426078081 CET	53	58730	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:54.448937893 CET	53830	53	192.168.2.6	8.8.4.4
Feb 23, 2021 17:08:54.511286974 CET	53	53830	8.8.4.4	192.168.2.6
Feb 23, 2021 17:08:54.559159994 CET	57226	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:54.607866049 CET	53	57226	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:58.703872919 CET	57880	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:58.766043901 CET	53	57880	8.8.8.8	192.168.2.6
Feb 23, 2021 17:08:58.803178072 CET	60850	53	192.168.2.6	8.8.4.4
Feb 23, 2021 17:08:58.853256941 CET	53	60850	8.8.4.4	192.168.2.6
Feb 23, 2021 17:08:58.889539957 CET	53187	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:08:58.946597099 CET	53	53187	8.8.8.8	192.168.2.6
Feb 23, 2021 17:09:18.081855059 CET	55830	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:09:18.132375002 CET	53	55830	8.8.8.8	192.168.2.6
Feb 23, 2021 17:09:18.138544083 CET	55145	53	192.168.2.6	8.8.4.4
Feb 23, 2021 17:09:18.192625999 CET	53	55145	8.8.4.4	192.168.2.6
Feb 23, 2021 17:09:18.249293089 CET	64091	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:09:18.298755884 CET	53	64091	8.8.8.8	192.168.2.6
Feb 23, 2021 17:09:22.310697079 CET	55728	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:09:22.370294094 CET	53	55728	8.8.8.8	192.168.2.6
Feb 23, 2021 17:09:22.370918989 CET	55694	53	192.168.2.6	8.8.4.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:09:22.430849075 CET	53	55694	8.8.4.4	192.168.2.6
Feb 23, 2021 17:09:22.432777882 CET	53926	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:09:22.483623028 CET	53	53926	8.8.8.8	192.168.2.6
Feb 23, 2021 17:09:26.499460936 CET	65531	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:09:26.561022043 CET	53	65531	8.8.8.8	192.168.2.6
Feb 23, 2021 17:09:26.561774015 CET	65437	53	192.168.2.6	8.8.4.4
Feb 23, 2021 17:09:26.613244057 CET	53	65437	8.8.4.4	192.168.2.6
Feb 23, 2021 17:09:26.616223097 CET	54590	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:09:26.664876938 CET	53	54590	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:07:24.744170904 CET	192.168.2.6	8.8.8.8	0x9f4f	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:24.857589960 CET	192.168.2.6	8.8.4.4	0x52e2	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:25.070523024 CET	192.168.2.6	8.8.8.8	0xe424	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:29.333532095 CET	192.168.2.6	8.8.8.8	0xc47e	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:29.421070099 CET	192.168.2.6	8.8.4.4	0xf758	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:29.498599052 CET	192.168.2.6	8.8.8.8	0x6d7c	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:33.832477093 CET	192.168.2.6	8.8.8.8	0x151d	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:33.941015005 CET	192.168.2.6	8.8.4.4	0x4a5b	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:34.048948050 CET	192.168.2.6	8.8.8.8	0xcb8c	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:53.348172903 CET	192.168.2.6	8.8.8.8	0x84cf	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:53.441025019 CET	192.168.2.6	8.8.4.4	0x4a7c	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:53.530246973 CET	192.168.2.6	8.8.8.8	0x6d7f	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:57.711498976 CET	192.168.2.6	8.8.8.8	0xf21d	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:57.802349091 CET	192.168.2.6	8.8.4.4	0x488f	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:57.914513111 CET	192.168.2.6	8.8.8.8	0x51da	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:02.050817013 CET	192.168.2.6	8.8.8.8	0x6778	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:02.114079952 CET	192.168.2.6	8.8.4.4	0x5c7	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:02.210747957 CET	192.168.2.6	8.8.8.8	0x6615	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:21.794615984 CET	192.168.2.6	8.8.8.8	0xc3cc	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:21.848858118 CET	192.168.2.6	8.8.4.4	0x1ea2	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:22.043221951 CET	192.168.2.6	8.8.8.8	0x67b1	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:26.147032976 CET	192.168.2.6	8.8.8.8	0xceb8	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:26.210582018 CET	192.168.2.6	8.8.4.4	0xf683	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:26.447410107 CET	192.168.2.6	8.8.8.8	0x4b3a	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:30.565412045 CET	192.168.2.6	8.8.8.8	0x253	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:30.700958967 CET	192.168.2.6	8.8.4.4	0xbbe3	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:30.804845095 CET	192.168.2.6	8.8.8.8	0x60e3	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:50.045794964 CET	192.168.2.6	8.8.8.8	0x91f7	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:50.103560925 CET	192.168.2.6	8.8.4.4	0xed9f	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:50.245938063 CET	192.168.2.6	8.8.8.8	0x6155	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)

Copyright null 2021

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:08:54.377499104 CET	192.168.2.6	8.8.8.8	0x8d4a	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:54.448937893 CET	192.168.2.6	8.8.4.4	0xc2a6	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:54.559159994 CET	192.168.2.6	8.8.8.8	0xfa62	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:58.703872919 CET	192.168.2.6	8.8.8.8	0x9eeb	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:58.803178072 CET	192.168.2.6	8.8.4.4	0x21cd	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:58.889539957 CET	192.168.2.6	8.8.8.8	0x8dc	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:18.081855059 CET	192.168.2.6	8.8.8.8	0xf0f9	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:18.138544083 CET	192.168.2.6	8.8.4.4	0x8dd1	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:18.249293089 CET	192.168.2.6	8.8.8.8	0x3894	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:22.310697079 CET	192.168.2.6	8.8.8.8	0xdf0c	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:22.370918989 CET	192.168.2.6	8.8.4.4	0x629c	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:22.432777882 CET	192.168.2.6	8.8.8.8	0x4535	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:26.499460936 CET	192.168.2.6	8.8.8.8	0xa039	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:26.561774015 CET	192.168.2.6	8.8.4.4	0xf620	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:26.616223097 CET	192.168.2.6	8.8.8.8	0x1517	Standard query (0)	kene3210.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:07:24.809181929 CET	8.8.8.8	192.168.2.6	0x9f4f	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:24.921189070 CET	8.8.4.4	192.168.2.6	0x52e2	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:25.199552059 CET	8.8.8.8	192.168.2.6	0xe424	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:29.393665075 CET	8.8.8.8	192.168.2.6	0xc47e	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:29.481549025 CET	8.8.4.4	192.168.2.6	0xf758	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:29.550241947 CET	8.8.8.8	192.168.2.6	0x6d7c	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:33.893160105 CET	8.8.8.8	192.168.2.6	0x151d	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:33.998241901 CET	8.8.4.4	192.168.2.6	0x4a5b	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:34.112571955 CET	8.8.8.8	192.168.2.6	0xcb8c	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:53.410068989 CET	8.8.8.8	192.168.2.6	0x84cf	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:53.489680052 CET	8.8.4.4	192.168.2.6	0x4a7c	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:53.582711935 CET	8.8.8.8	192.168.2.6	0x6d7f	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:57.773730993 CET	8.8.8.8	192.168.2.6	0xf21d	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)

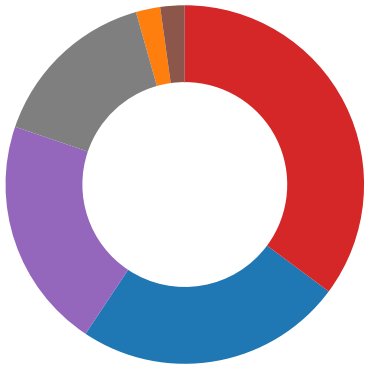
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:07:57.853434086 CET	8.8.4.4	192.168.2.6	0x488f	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:07:57.973037004 CET	8.8.8.8	192.168.2.6	0x51da	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:02.110687017 CET	8.8.8.8	192.168.2.6	0x6778	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:02.172787905 CET	8.8.4.4	192.168.2.6	0x5c7	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:02.268100977 CET	8.8.8.8	192.168.2.6	0x6615	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:21.844912052 CET	8.8.8.8	192.168.2.6	0xc3cc	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:21.899621010 CET	8.8.4.4	192.168.2.6	0x1ea2	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:22.100816965 CET	8.8.8.8	192.168.2.6	0x67b1	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:26.204144955 CET	8.8.8.8	192.168.2.6	0xceb8	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:26.262346029 CET	8.8.4.4	192.168.2.6	0xf683	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:26.512365103 CET	8.8.8.8	192.168.2.6	0x4b3a	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:30.624352932 CET	8.8.8.8	192.168.2.6	0x253	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:30.752542973 CET	8.8.4.4	192.168.2.6	0xbbe3	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:30.861898899 CET	8.8.8.8	192.168.2.6	0x60e3	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:50.100102901 CET	8.8.8.8	192.168.2.6	0x91f7	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:50.153879881 CET	8.8.4.4	192.168.2.6	0xed9f	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:50.308901072 CET	8.8.8.8	192.168.2.6	0x6155	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:54.426078081 CET	8.8.8.8	192.168.2.6	0x8d4a	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:54.511286974 CET	8.8.4.4	192.168.2.6	0xc2a6	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:54.607866049 CET	8.8.8.8	192.168.2.6	0xfa62	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:58.766043901 CET	8.8.8.8	192.168.2.6	0x9eeb	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:58.853256941 CET	8.8.4.4	192.168.2.6	0x21cd	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:08:58.946597099 CET	8.8.8.8	192.168.2.6	0x8dc	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:18.132375002 CET	8.8.8.8	192.168.2.6	0xf0f9	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:18.192625999 CET	8.8.4.4	192.168.2.6	0x8dd1	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:18.298755884 CET	8.8.8.8	192.168.2.6	0x3894	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:09:22.370294094 CET	8.8.8.8	192.168.2.6	0xdf0c	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:22.430849075 CET	8.8.4.4	192.168.2.6	0x629c	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:22.483623028 CET	8.8.8.8	192.168.2.6	0x4535	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:26.561022043 CET	8.8.8.8	192.168.2.6	0xa039	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:26.613244057 CET	8.8.4.4	192.168.2.6	0xf620	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:09:26.664876938 CET	8.8.8.8	192.168.2.6	0x1517	Name error (3)	kene3210.ddns.net	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: UCDR562uYv.exe PID: 6804 Parent PID: 6068

General

Start time:	17:07:14
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\UCDR562uYv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\UCDR562uYv.exe'
Imagebase:	0xa30000
File size:	820224 bytes
MD5 hash:	CF3CBCF8EED33D5DD9778C4914B21FD9
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: 00000000.00000002.349423394.0000000004306000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.349423394.0000000004306000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.349423394.0000000004306000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.347500177.0000000003F51000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.347500177.0000000003F51000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.347500177.0000000003F51000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Roaming\IRvvjxua.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CD31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp483E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD37038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\UCDR562uYv.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1FC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp483E.tmp	success or wait	1	6CD36A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\lRvvjxua.exe	unknown	820224	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 b9 e2 6c ee 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 7a 0c 00 00 08 00 00 00 00 00 00 1a 98 0c 00 00 20 00 00 00 a0 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....l........... ....0..z............... ....@.. ....@.................	success or wait	1	6CD31B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp483E.tmp	unknown	1653	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10- 25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </Registratio	success or wait	1	6CD31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\UCDR562uYv.exe.log	unknown	1301	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	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_v4.0.3	success or wait	1	6E1FC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Users\user\Desktop\UCDR562uYv.exe	unknown	820224	success or wait	1	6CD31B4F	ReadFile

Analysis Process: schtasks.exe PID: 7000 Parent PID: 6804

General

Start time:	17:07:18
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lRvvjxua' /XML 'C:\Users\user\AppData\Local\Temp\tmp483E.tmp'
Imagebase:	0x13d0000
File size:	185856 bytes

MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp483E.tmp	unknown	2	success or wait	1	13DAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp483E.tmp	unknown	1654	success or wait	1	13DABD9	ReadFile

Analysis Process: conhost.exe PID: 7024 Parent PID: 7000

General

Start time:	17:07:18
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: UCDR562uYv.exe PID: 7060 Parent PID: 6804

General

Start time:	17:07:19
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\UCDR562uYv.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc80000
File size:	820224 bytes
MD5 hash:	CF3CBCF8EED33D5DD9778C4914B21FD9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright null 2021

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.599662311.0000000003181000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.604263829.00000000062B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.604263829.00000000062B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.604263829.00000000062B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.598230580.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.598230580.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.598230580.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.604092482.0000000005A90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.604092482.0000000005A90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.602748290.0000000004189000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.602748290.0000000004189000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CD31E60	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD3BEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CD3DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CD3DD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD3BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\UCDR562uYv.exe:Zone.Identifier	success or wait	1	6CCB2935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	46 41 56 8a 60 d8 d8 48	FAV.`..H	success or wait	1	6CD31B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 b9 e2 6c ee 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 7a 0c 00 00 08 00 00 00 00 00 00 1a 98 0c 00 00 20 00 00 00 a0 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....l........... ....0..z.............. ....@.. ....@................	success or wait	4	6CD3DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CD3DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile

Copyright null 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DEAD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DEAD72F	unknown
C:\Users\user\Desktop\UCDR562uYv.exe	unknown	4096	success or wait	1	6DEAD72F	unknown
C:\Users\user\Desktop\UCDR562uYv.exe	unknown	512	success or wait	1	6DEAD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6DEAD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6DEAD72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6CD3646A	RegSetValueExW

Analysis Process: dhcpmon.exe PID: 4964 Parent PID: 3440

General

Start time:	17:07:30
Start date:	23/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xea0000
File size:	820224 bytes
MD5 hash:	CF3CBCF8EED33D5DD9778C4914B21FD9
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: 00000008.00000002.384846526.0000000004656000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.384846526.0000000004656000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.384846526.0000000004656000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.384087909.00000000042A1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.384087909.00000000042A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.384087909.00000000042A1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Local\Temp\tmp86BE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD37038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1FC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp86BE.tmp	success or wait	1	6CD36A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp86BE.tmp	unknown	1653	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">..<RegistrationInfo>..<Date>2014-10-25T14:27:44.8929027</Date>..<Author>computer\user</Author>..</Registratio	success or wait	1	6CD31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	1301	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	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_v4.0.3	success or wait	1	6E1FC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile

Analysis Process: schtasks.exe PID: 6364 Parent PID: 4964

General

Start time:	17:07:36
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lRvvjxua' /XML 'C:\Users\user\AppData\Local\Temp\tmp86BE.tmp'
Imagebase:	0x13d0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp86BE.tmp	unknown	2	success or wait	1	13DAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp86BE.tmp	unknown	1654	success or wait	1	13DABD9	ReadFile

Analysis Process: conhost.exe PID: 6352 Parent PID: 6364

General

Start time:	17:07:36
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 6440 Parent PID: 4964

General

Start time:	17:07:37
Start date:	23/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xdd0000
File size:	820224 bytes
MD5 hash:	CF3CBCF8EED33D5DD9778C4914B21FD9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright null 2021

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.395887312.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.395887312.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.395887312.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.396942381.0000000003251000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.396942381.0000000003251000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.397040286.0000000004259000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.397040286.0000000004259000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile

Disassembly

Code Analysis