ID: 878809
Sample Name: 02399999.exe
Cookbook: default.jbs
Time: 08:32:57
Date: 31/05/2023
Version: 37.1.0 Beryl

Table of Contents

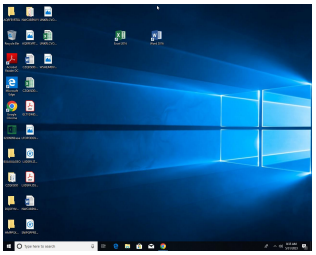
Windows Analysis Report

02399999.exe

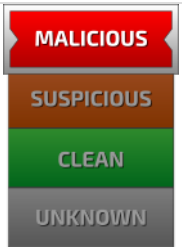
Overview

General Information

Sample Name:	02399999.exe
Analysis ID:	878809
MD5:	b2662708454e…
SHA1:	f1b651b571cd6..
SHA256:	c9c5e89d6da5…
Infos:	



Detection



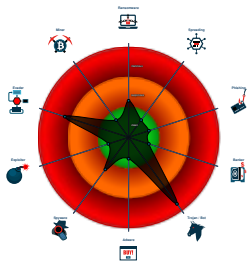
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Machine Learning detection for drop…

Classification



Process Tree

- **System is w10x64**
- 02399999.exe (PID: 7264 cmdline: C:\Users\user\Desktop\02399999.exe MD5: B2662708454EC2456F52DB8B237C6C33)
- dhcpmon.exe (PID: 7360 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: B2662708454EC2456F52DB8B237C6C33)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Nanocore RAT, NanoCore	Nanocore is a Remote Access Tool used to steal credentials and to spy on cameras. It as been used for a while by numerous criminal actors as well as by nation state threat actors.	• APT33 • The Gorgon Group	**http://** https://assets.virustotal.com/reports/2021trends.pdfhttps://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/https://blog.morphisec.com/syk-crypter-discord	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.nanocore

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "b4f3dcf4-de9c-48f4-bd4e-55544002",
  "Group": "Clients",
  "Domain1": "45.35.64.214",
  "Domain2": "168.119.0.173",
  "Port": 5665,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 3000,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "1.1.1.1",
  "BackupDNSServer": "8.8.8.8"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
02399999.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
02399999.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
02399999.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
02399999.exe	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xfef5:$x1: NanoCore Client • 0xff05:$x1: NanoCore Client • 0x1014d:$x2: NanoCore.ClientPlugin • 0x1018d:$x3: NanoCore.ClientPluginHost • 0x10142:$i1: IClientApp • 0x10163:$i2: IClientData • 0x1016f:$i3: IClientNetwork • 0x1017e:$i4: IClientAppHost • 0x101a7:$i5: IClientDataHost • 0x101b7:$i6: IClientLoggingHost • 0x101ca:$i7: IClientNetworkHost • 0x101dd:$i8: IClientUIHost • 0x101eb:$i9: IClientNameObjectCollection • 0x10207:$i10: IClientReadOnlyNameObjectCollection • 0xff54:$s1: ClientPlugin • 0x10156:$s1: ClientPlugin • 0x1064a:$s2: EndPoint • 0x10653:$s3: IPAddress • 0x1065d:$s4: IPEndPoint • 0x12093:$s6: get_ClientSettings • 0x12637:$s7: get_Connected

Source	Rule	Description	Author	Strings
02399999.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
Click to see the 1 entries				

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xfef5:$x1: NanoCore Client • 0xff05:$x1: NanoCore Client • 0x1014d:$x2: NanoCore.ClientPlugin • 0x1018d:$x3: NanoCore.ClientPluginHost • 0x10142:$i1: IClientApp • 0x10163:$i2: IClientData • 0x1016f:$i3: IClientNetwork • 0x1017e:$i4: IClientAppHost • 0x101a7:$i5: IClientDataHost • 0x101b7:$i6: IClientLoggingHost • 0x101ca:$i7: IClientNetworkHost • 0x101dd:$i8: IClientUIHost • 0x101eb:$i9: IClientNameObjectCollection • 0x10207:$i10: IClientReadOnlyNameObjectCollection • 0xff54:$s1: ClientPlugin • 0x10156:$s1: ClientPlugin • 0x1064a:$s2: EndPoint • 0x10653:$s3: IPAddress • 0x1065d:$s4: IPEndPoint • 0x12093:$s6: get_ClientSettings • 0x12637:$s7: get_Connected
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.637694983.0000000005C60000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000000.00000002.637694983.0000000005C60000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000000.00000002.637694983.0000000005C60000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.637694983.0000000005C60000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xf778:$x2: NanoCore.ClientPlugin • 0xf7ad:$x3: NanoCore.ClientPluginHost • 0xf76c:$i2: IClientData • 0xf78e:$i3: IClientNetwork • 0xf79d:$i5: IClientDataHost • 0xf7c7:$i6: IClientLoggingHost • 0xf7da:$i7: IClientNetworkHost • 0xf7ed:$i8: IClientUIHost • 0xf7fb:$i9: IClientNameObjectCollection • 0xf817:$i10: IClientReadOnlyNameObjectCollection • 0xf56a:$s1: ClientPlugin • 0xf781:$s1: ClientPlugin • 0x147a2:$s6: get_ClientSettings
00000000.00000002.637694983.0000000005C60000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xf7ad:$a1: NanoCore.ClientPluginHost • 0xf778:$a2: NanoCore.ClientPlugin • 0x146f3:$b1: get_BuilderSettings • 0x14662:$b7: LogClientException • 0xf7c7:$b9: IClientLoggingHost
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.dhcpmon.exe.400e44c.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
1.2.dhcpmon.exe.400e44c.1.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
1.2.dhcpmon.exe.400e44c.1.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
1.2.dhcpmon.exe.400e44c.1.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xd978:$x2: NanoCore.ClientPlugin • 0xd9ad:$x3: NanoCore.ClientPluginHost • 0xd96c:$i2: IClientData • 0xd98e:$i3: IClientNetwork • 0xd99d:$i5: IClientDataHost • 0xd9c7:$i6: IClientLoggingHost • 0xd9da:$i7: IClientNetworkHost • 0xd9ed:$i8: IClientUIHost • 0xd9fb:$i9: IClientNameObjectCollection • 0xda17:$i10: IClientReadOnlyNameObjectCollection • 0xd76a:$s1: ClientPlugin • 0xd981:$s1: ClientPlugin • 0x129a2:$s6: get_ClientSettings
1.2.dhcpmon.exe.400e44c.1.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xd9ad:$a1: NanoCore.ClientPluginHost • 0xd978:$a2: NanoCore.ClientPlugin • 0x128f3:$b1: get_BuilderSettings • 0x12862:$b7: LogClientException • 0xd9c7:$b9: IClientLoggingHost
Click to see the 49 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

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

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

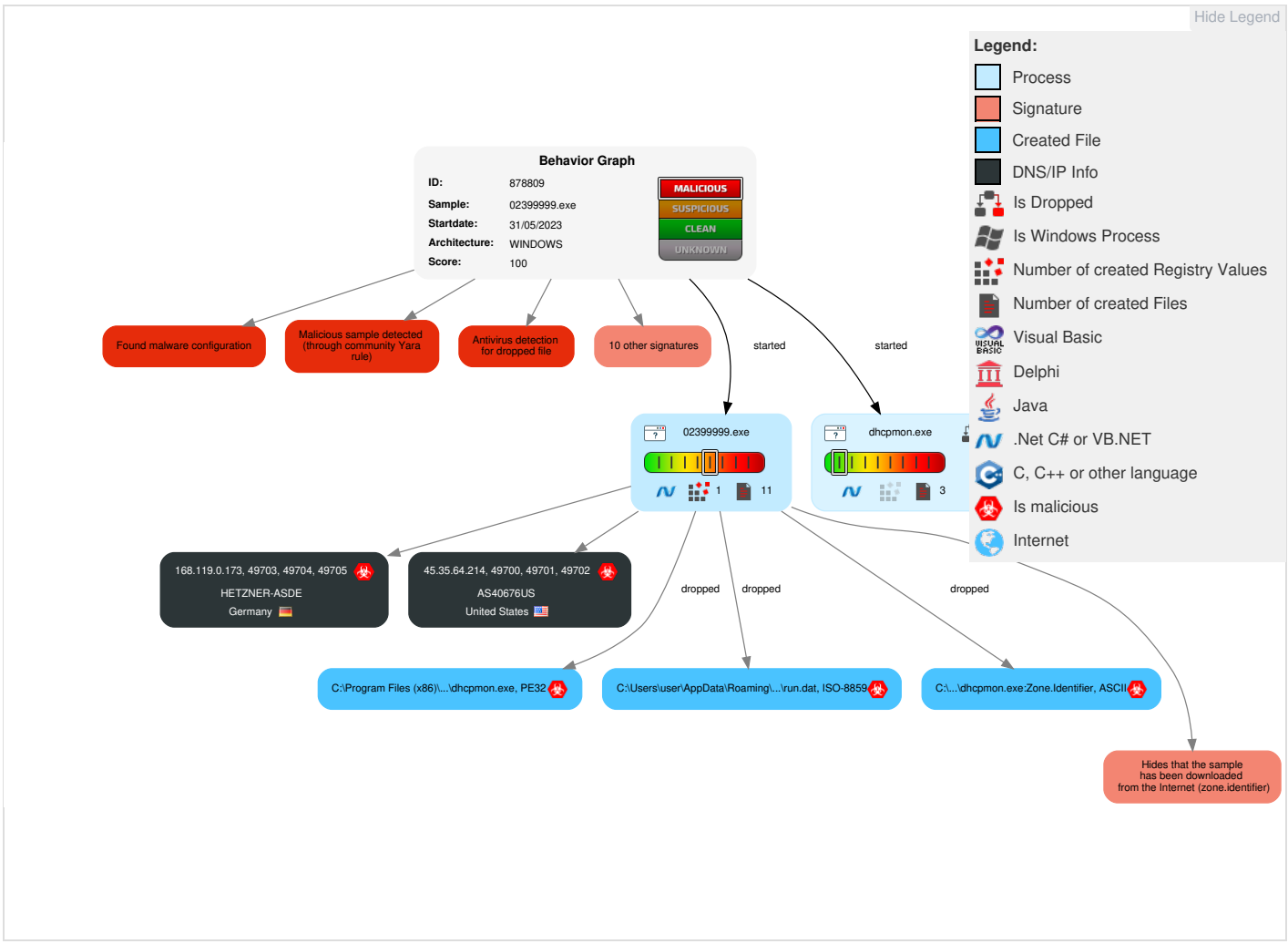
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Access Token Manipulation	2 Masquerading	2 1 Input Capture	1 1 Security Software Discovery	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	2 Process Injection	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Access Token Manipulation	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Process Injection	LSA Secrets	3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Hidden Files and Directories	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

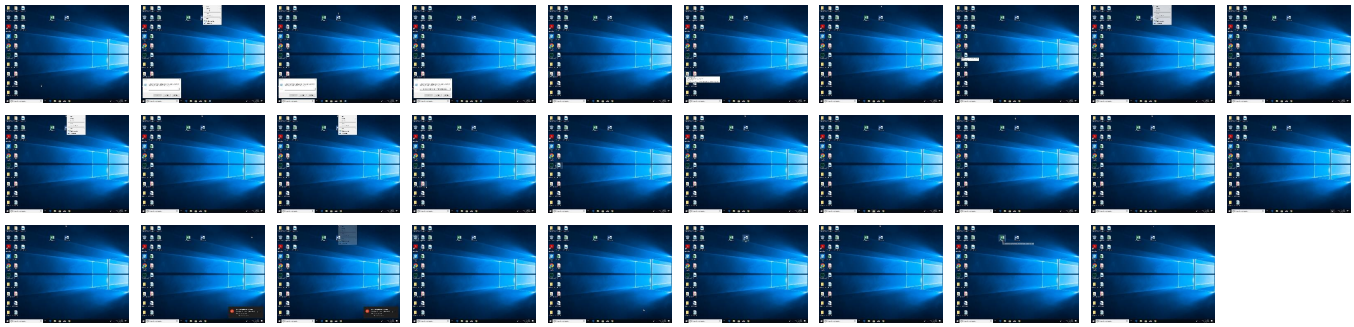
Behavior Graph



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
02399999.exe	97%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
02399999.exe	85%	Virustotal		Browse
02399999.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
02399999.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	97%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
168.119.0.173	0%	Avira URL Cloud	safe	
45.35.64.214	0%	Avira URL Cloud	safe	
45.35.64.214	0%	Virustotal		Browse

Domains and IPs

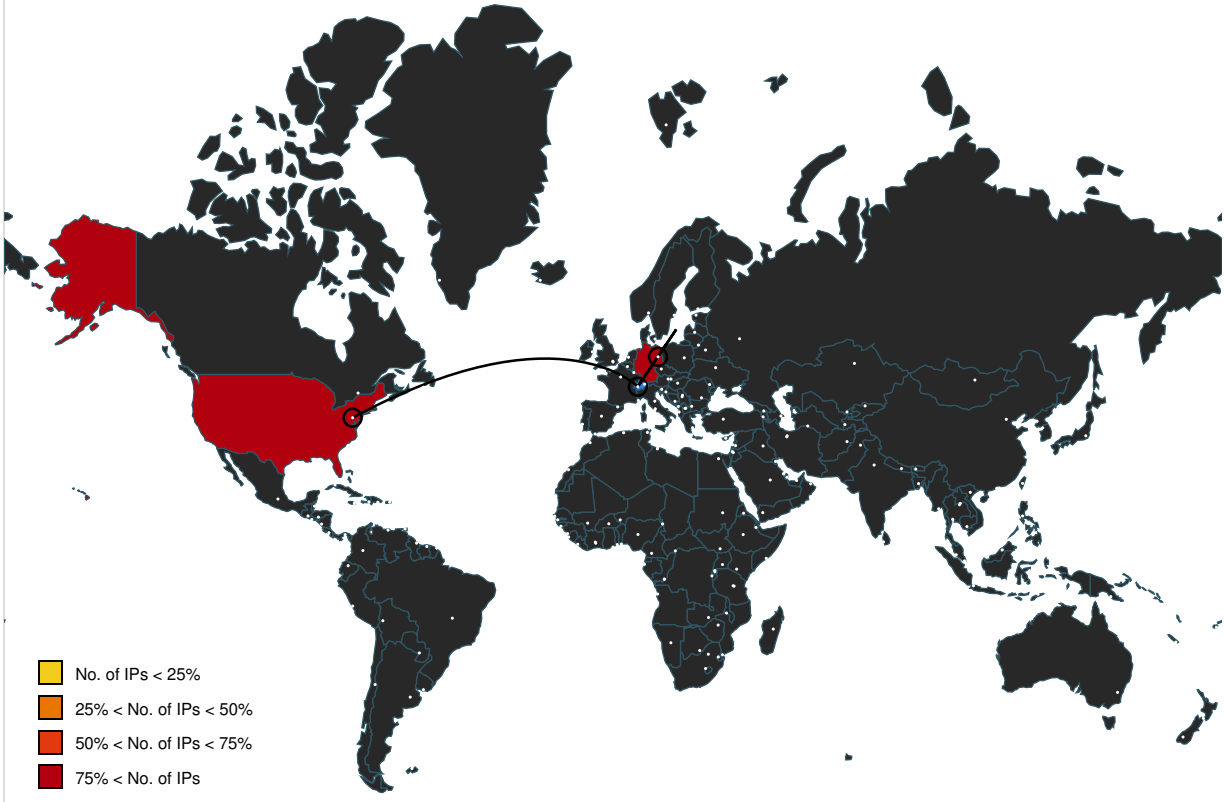
Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
168.119.0.173	true	• Avira URL Cloud: safe	unknown
45.35.64.214	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
168.119.0.173	unknown	Germany		24940	HETZNER-ASDE	true
45.35.64.214	unknown	United States		40676	AS40676US	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	878809
Start date and time:	2023-05-31 08:32:57 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	6
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
Sample file name:	02399999.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@2/4@0/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:33:53	API Interceptor	912x Sleep call for process: 02399999.exe modified
08:33:55	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

ASNs

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\02399999.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	307712
Entropy (8bit):	6.3535462402853815
Encrypted:	false
SSDEEP:	6144:2LV6Bta6dtJmakIM50Qm2bTnvHbLOupQe4li2+m:2LV6BtpmkzizzLVpEs2+m
MD5:	B2662708454EC2456F52DB8B237C6C33
SHA1:	F1B651B571CD6A7CA9A2939DF25B5ECCA440C065
SHA-256:	C9C5E89D6DA5C9DA9CC6244BE14270A8730604BBD55C78D005FD24D6C9714299
SHA-512:	D9DA7810C285E9B144533A7C745950B1CDB94F91B39907F3F02300DAA01B072DB27C951043FDE9BF9BC0AE81FD9D3D2D2A7949122A0C073757384987089D04B
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 97%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T..... .....@.. ....8...W.... ..T..... ....H.....text..... ....`.reloc.....@..B.rsrc...T.... .....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s 8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$..... ~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

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

Process:	C:\Users\user\Desktop\02399999.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

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

Process:	C:\Users\user\Desktop\02399999.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:j6KSn:bS
MD5:	517910715AD0616C991340E985EE5A30
SHA1:	C72167B42DF345BA5542169A3056C48A45DBF247
SHA-256:	33102EC4FADC6613E85AC2EFC21B6FED2FB9417B9F6710A15B85344C69A7EF9F
SHA-512:	B2D278474833EF3D5BA6D0C2416F8A1969168FB8F4A57E1ED6A4BCBC11FE4BD4C28237EC07FFE9B08022C5CF2DD5E45A99FB465DCD4F0B531F1568190E3A29AB
Malicious:	**true**
Preview:	...p.a.H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.3535462402853815
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	02399999.exe
File size:	307712
MD5:	b2662708454ec2456f52db8b237c6c33
SHA1:	f1b651b571cd6a7ca9a2939df25b5ecca440c065
SHA256:	c9c5e89d6da5c9da9cc6244be14270a8730604bbd55c78d005fd24d6c9714299
SHA512:	d9da7810c285e9b144533a7c745950b1cdb94f91b39907f3f02300daa01b072db27c951043fde9bf9bc0ae81fd9d3d2d2a7949122a0c073757384987089d04b7
SSDEEP:	6144:2LV6Bta6dtJmakIM50Qm2bTnvHbLOupQe4li2+m:2LV6BtpmkzizzLVpEs2+m
TLSH:	21649D0522B1891EE28E85FB60D1410247B9C9DA9ADFF3DE78B079B65B732D211473E3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T..... .....@.. ....

File Icon

Icon Hash:	03181a5216dcd826

Static PE Info

General

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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1e738	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x22000	0x2e454	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x20000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x1c798	0x1c800	False	0.5945124040570176	data	6.598081105091412	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x2e454	0x2e600	False	0.49973151111859837	data	5.889564453885382	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x221a8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024, resolution 2835 x 2835 px/m		
RT_ICON	0x22610	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216, resolution 2835 x 2835 px/m		
RT_ICON	0x24bb8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096, resolution 2835 x 2835 px/m		
RT_ICON	0x25c60	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536, resolution 2835 x 2835 px/m		
RT_ICON	0x36488	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384, resolution 2835 x 2835 px/m		
RT_RCDATA	0x3a6b0	0x15d48	data		
RT_GROUP_ICON	0x503f8	0x5a	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

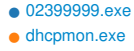
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 08:33:55.751533985 CEST	49700	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:33:55.895180941 CEST	5665	49700	45.35.64.214	192.168.2.3
May 31, 2023 08:33:56.404943943 CEST	49700	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:33:56.547894001 CEST	5665	49700	45.35.64.214	192.168.2.3
May 31, 2023 08:33:57.061247110 CEST	49700	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:33:57.204063892 CEST	5665	49700	45.35.64.214	192.168.2.3
May 31, 2023 08:34:01.266536951 CEST	49701	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:34:01.408772945 CEST	5665	49701	45.35.64.214	192.168.2.3
May 31, 2023 08:34:01.921174049 CEST	49701	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:34:02.063179016 CEST	5665	49701	45.35.64.214	192.168.2.3
May 31, 2023 08:34:02.577311039 CEST	49701	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:34:02.719145060 CEST	5665	49701	45.35.64.214	192.168.2.3
May 31, 2023 08:34:06.737678051 CEST	49702	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:34:06.881084919 CEST	5665	49702	45.35.64.214	192.168.2.3
May 31, 2023 08:34:07.390307903 CEST	49702	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:34:07.533823013 CEST	5665	49702	45.35.64.214	192.168.2.3
May 31, 2023 08:34:08.046559095 CEST	49702	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:34:08.190159082 CEST	5665	49702	45.35.64.214	192.168.2.3
May 31, 2023 08:34:12.235112906 CEST	49703	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:12.257488966 CEST	5665	49703	168.119.0.173	192.168.2.3
May 31, 2023 08:34:12.765901089 CEST	49703	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:12.788434029 CEST	5665	49703	168.119.0.173	192.168.2.3
May 31, 2023 08:34:13.298998117 CEST	49703	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:13.321403027 CEST	5665	49703	168.119.0.173	192.168.2.3
May 31, 2023 08:34:17.338488102 CEST	49704	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:17.361402988 CEST	5665	49704	168.119.0.173	192.168.2.3
May 31, 2023 08:34:17.876277924 CEST	49704	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:17.899055958 CEST	5665	49704	168.119.0.173	192.168.2.3
May 31, 2023 08:34:18.406825066 CEST	49704	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:18.429586887 CEST	5665	49704	168.119.0.173	192.168.2.3
May 31, 2023 08:34:22.486254930 CEST	49705	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:22.508563042 CEST	5665	49705	168.119.0.173	192.168.2.3
May 31, 2023 08:34:23.016665936 CEST	49705	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:23.041065931 CEST	5665	49705	168.119.0.173	192.168.2.3
May 31, 2023 08:34:23.547848940 CEST	49705	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:23.570111036 CEST	5665	49705	168.119.0.173	192.168.2.3
May 31, 2023 08:34:27.827264071 CEST	49706	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:34:27.969439983 CEST	5665	49706	45.35.64.214	192.168.2.3
May 31, 2023 08:34:28.548422098 CEST	49706	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:34:28.690658092 CEST	5665	49706	45.35.64.214	192.168.2.3
May 31, 2023 08:34:29.360943079 CEST	49706	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:34:29.503098965 CEST	5665	49706	45.35.64.214	192.168.2.3
May 31, 2023 08:34:33.518711090 CEST	49707	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:34:33.660736084 CEST	5665	49707	45.35.64.214	192.168.2.3
May 31, 2023 08:34:34.173868895 CEST	49707	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:34:34.315943956 CEST	5665	49707	45.35.64.214	192.168.2.3
May 31, 2023 08:34:34.830133915 CEST	49707	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:34:34.972138882 CEST	5665	49707	45.35.64.214	192.168.2.3
May 31, 2023 08:34:38.996997118 CEST	49708	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:34:39.139564037 CEST	5665	49708	45.35.64.214	192.168.2.3
May 31, 2023 08:34:39.643038988 CEST	49708	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:34:39.786314964 CEST	5665	49708	45.35.64.214	192.168.2.3
May 31, 2023 08:34:40.299324989 CEST	49708	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:34:40.449640989 CEST	5665	49708	45.35.64.214	192.168.2.3
May 31, 2023 08:34:45.254376888 CEST	49709	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:45.277055025 CEST	5665	49709	168.119.0.173	192.168.2.3
May 31, 2023 08:34:45.909198046 CEST	49709	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:45.934518099 CEST	5665	49709	168.119.0.173	192.168.2.3
May 31, 2023 08:34:46.612446070 CEST	49709	5665	192.168.2.3	168.119.0.173

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 08:34:46.635319948 CEST	5665	49709	168.119.0.173	192.168.2.3
May 31, 2023 08:34:50.652786016 CEST	49710	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:50.675084114 CEST	5665	49710	168.119.0.173	192.168.2.3
May 31, 2023 08:34:51.175255060 CEST	49710	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:51.197210073 CEST	5665	49710	168.119.0.173	192.168.2.3
May 31, 2023 08:34:51.706621885 CEST	49710	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:51.728646994 CEST	5665	49710	168.119.0.173	192.168.2.3
May 31, 2023 08:34:55.740019083 CEST	49711	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:55.762631893 CEST	5665	49711	168.119.0.173	192.168.2.3
May 31, 2023 08:34:56.270252943 CEST	49711	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:56.292642117 CEST	5665	49711	168.119.0.173	192.168.2.3
May 31, 2023 08:34:56.800751925 CEST	49711	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:34:56.823265076 CEST	5665	49711	168.119.0.173	192.168.2.3
May 31, 2023 08:35:00.964832067 CEST	49712	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:35:01.109076977 CEST	5665	49712	45.35.64.214	192.168.2.3
May 31, 2023 08:35:01.613913059 CEST	49712	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:35:01.758080006 CEST	5665	49712	45.35.64.214	192.168.2.3
May 31, 2023 08:35:02.270045042 CEST	49712	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:35:02.414397955 CEST	5665	49712	45.35.64.214	192.168.2.3
May 31, 2023 08:35:06.503844023 CEST	49713	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:35:06.647836924 CEST	5665	49713	45.35.64.214	192.168.2.3
May 31, 2023 08:35:07.161165953 CEST	49713	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:35:07.305179119 CEST	5665	49713	45.35.64.214	192.168.2.3
May 31, 2023 08:35:07.817339897 CEST	49713	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:35:07.961353064 CEST	5665	49713	45.35.64.214	192.168.2.3
May 31, 2023 08:35:11.974648952 CEST	49714	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:35:12.119107008 CEST	5665	49714	45.35.64.214	192.168.2.3
May 31, 2023 08:35:12.630232096 CEST	49714	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:35:12.774909973 CEST	5665	49714	45.35.64.214	192.168.2.3
May 31, 2023 08:35:13.286627054 CEST	49714	5665	192.168.2.3	45.35.64.214
May 31, 2023 08:35:13.430577040 CEST	5665	49714	45.35.64.214	192.168.2.3
May 31, 2023 08:35:17.460676908 CEST	49715	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:35:17.483330011 CEST	5665	49715	168.119.0.173	192.168.2.3
May 31, 2023 08:35:17.990077019 CEST	49715	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:35:18.014878035 CEST	5665	49715	168.119.0.173	192.168.2.3
May 31, 2023 08:35:18.517863989 CEST	49715	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:35:18.540355921 CEST	5665	49715	168.119.0.173	192.168.2.3
May 31, 2023 08:35:22.546876907 CEST	49716	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:35:22.569528103 CEST	5665	49716	168.119.0.173	192.168.2.3
May 31, 2023 08:35:23.075854063 CEST	49716	5665	192.168.2.3	168.119.0.173
May 31, 2023 08:35:23.098355055 CEST	5665	49716	168.119.0.173	192.168.2.3

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 02399999.exe PID: **7264**, Parent PID: **3452**

General

Target ID:	0
Start time:	08:33:49
Start date:	31/05/2023
Path:	C:\Users\user\Desktop\02399999.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\02399999.exe
Imagebase:	0xd40000
File size:	307712 bytes
MD5 hash:	B2662708454EC2456F52DB8B237C6C33
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: 00000000.00000002.637694983.0000000005C60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.637694983.0000000005C60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.637694983.0000000005C60000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.637694983.0000000005C60000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.637694983.0000000005C60000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000000.359925948.0000000000D42000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.359925948.0000000000D42000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.359925948.0000000000D42000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000000.359925948.0000000000D42000.00000002.00000001.01000000.00000003.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.631551849.00000000034A1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.637488624.00000000058C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.637488624.00000000058C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.637488624.00000000058C0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.637488624.00000000058C0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
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	6C8660AC	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	6C8660AC	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	3040D15	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	3040E0F	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	3040D15	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	3041094	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	3041094	CopyFileW
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	3040D15	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	3040D15	CreateDirectoryW
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	6C8660AC	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	6C8660AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\02399999.exe:Zone.Identifier	success or wait	1	3041265	DeleteFileA

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	0	8	fd fd fd 70 fd 61 fd 48	paH	success or wait	1	3040FC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 27 fd 54 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 fd 01 00 00 fd 02 00 00 00 00 00 fd fd 01 00 00 20 00 00 00 00 02 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 20 05 00 00 02 00 00 00 00 00 00 02 00 00 00 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.$PEL'T @	success or wait	3	3041094	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	3041094	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C895544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C895544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C898738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6C93BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6C93BF06	unknown
C:\Users\user\Desktop\02399999.exe	unknown	4096	success or wait	1	6C93BF06	unknown
C:\Users\user\Desktop\02399999.exe	unknown	512	success or wait	1	6C93BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C895544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	6C895544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	3040FC7	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	3040FC7	ReadFile

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	3041186	RegSetValueExW

Analysis Process: dhcpmon.exe PID: **7360**, Parent PID: **3452**

General

Target ID:	1

Start time:	08:34:04
Start date:	31/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x8f0000
File size:	307712 bytes
MD5 hash:	B2662708454EC2456F52DB8B237C6C33
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.408989152.0000000003FC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.408989152.0000000003FC1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.408989152.0000000003FC1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.408896895.0000000002FC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.408896895.0000000002FC1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.408896895.0000000002FC1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 97%, ReversingLabs
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	6C8660AC	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	6C8660AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C8534A7	CreateFileW

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\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	0	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",03,"	success or wait	1	6CB3A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C895544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C895544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C898738	ReadFile

Disassembly

No disassembly