ID: 433324
Sample Name: PAYMENT-PO#45678.exe
Cookbook: default.jbs
Time: 16:32:21
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

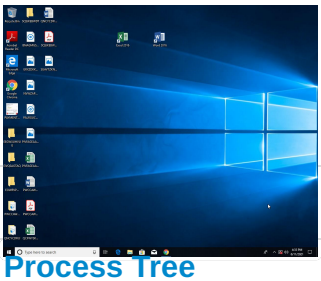
Analysis Report PAYMENT-PO#45678.exe

Overview

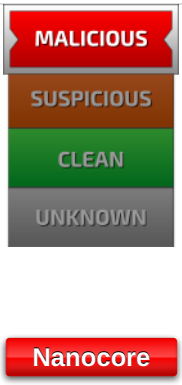
General Information

Sample Name:	PAYMENT-PO#45678.exe
Analysis ID:	433324
MD5:	438425f009b3731.
SHA1:	5f686134a72fe12..
SHA256:	b2262126a955e3..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

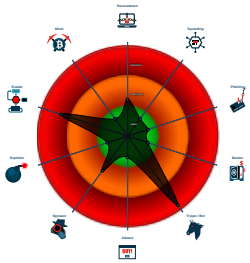


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …

Classification



Process Tree

- **System is w10x64**
- PAYMENT-PO#45678.exe (PID: 6600 cmdline: 'C:\Users\user\Desktop\PAYMENT-PO#45678.exe' MD5: 438425F009B373154E4E3629C3539581)
  - PAYMENT-PO#45678.exe (PID: 6688 cmdline: C:\Users\user\Desktop\PAYMENT-PO#45678.exe MD5: 438425F009B373154E4E3629C3539581)
  - PAYMENT-PO#45678.exe (PID: 6736 cmdline: C:\Users\user\Desktop\PAYMENT-PO#45678.exe MD5: 438425F009B373154E4E3629C3539581)
    - schtasks.exe (PID: 6788 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp8E26.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6800 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6844 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp91A2.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- PAYMENT-PO#45678.exe (PID: 6920 cmdline: C:\Users\user\Desktop\PAYMENT-PO#45678.exe 0 MD5: 438425F009B373154E4E3629C3539581)
  - PAYMENT-PO#45678.exe (PID: 7020 cmdline: C:\Users\user\Desktop\PAYMENT-PO#45678.exe MD5: 438425F009B373154E4E3629C3539581)
- dhcpmon.exe (PID: 6968 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 438425F009B373154E4E3629C3539581)
  - dhcpmon.exe (PID: 7040 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 438425F009B373154E4E3629C3539581)
- dhcpmon.exe (PID: 4952 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 438425F009B373154E4E3629C3539581)
  - dhcpmon.exe (PID: 6340 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 438425F009B373154E4E3629C3539581)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "fa01d1ff-8193-42b2-a0e1-b0e6c90b",
  "Group": "PO-#9874567",
  "Domain1": "doc-file.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 7755,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "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",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.240871445.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000B.00000002.240871445.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000B.00000002.240871445.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000009.00000002.227725816.000000000464000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x9c12d:$x1: NanoCore.ClientPluginHost • 0x9c16a:$x2: IClientNetworkHost • 0x9fc9d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000009.00000002.227725816.000000000464000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 108 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PAYMENT-PO#45678.exe.46e1fa0.11.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.PAYMENT-PO#45678.exe.46e1fa0.11.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
0.2.PAYMENT-PO#45678.exe.46e1fa0.11.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.PAYMENT-PO#45678.exe.46e1fa0.11.raw.unpack	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:$j: #=q
13.2.dhcpmon.exe.2c9cd34.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 223 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

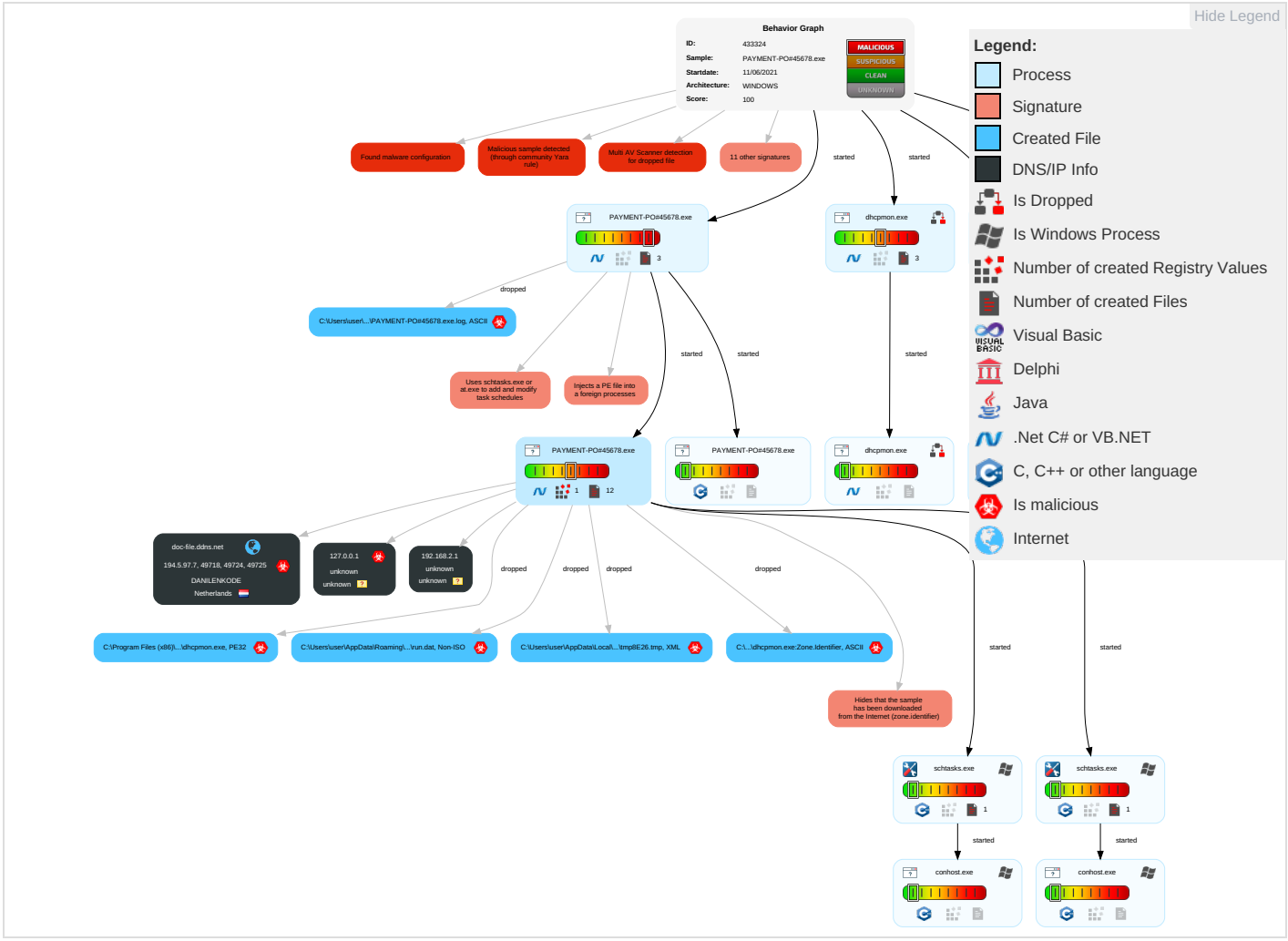
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 2	Input Capture 2 1	Security Software Discovery 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

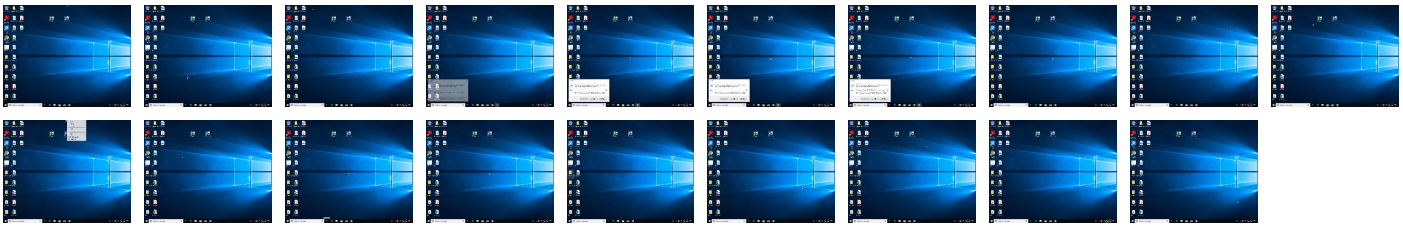
Behavior Graph



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
PAYMENT-PO#45678.exe	41%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
PAYMENT-PO#45678.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	41%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.0.PAYMENT-PO#45678.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.dhcpmon.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.dhcpmon.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.2.PAYMENT-PO#45678.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.PAYMENT-PO#45678.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.dhcpmon.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.PAYMENT-PO#45678.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.PAYMENT-PO#45678.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.PAYMENT-PO#45678.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.PAYMENT-PO#45678.exe.5540000.10.unpack	100%	Avira	TR/NanoCore.fadte		Download File
11.0.dhcpmon.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
doc-file.ddns.net	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
doc-file.ddns.net	3%	Virustotal		Browse
doc-file.ddns.net	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Virustotal		Browse
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
doc-file.ddns.net	194.5.97.7	true	true	• 3%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
doc-file.ddns.net	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
127.0.0.1	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.97.7	doc-file.ddns.net	Netherlands		208476	DANILENKODE	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433324
Start date:	11.06.2021
Start time:	16:32:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PAYMENT-PO#45678.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:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@20/8@12/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.3%) • Quality average: 56.5% • Quality standard deviation: 32.5%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:33:14	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\PAYMENT-PO#45678.exe" s>$(Arg0)
16:33:14	API Interceptor	1032x Sleep call for process: PAYMENT-PO#45678.exe modified
16:33:14	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
16:33:15	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.97.7	PAYMENT-PO#987654567.exe	Get hash	malicious	Browse	
	8RJwUlmBjb.exe	Get hash	malicious	Browse	
	B882ITuiXnqLLeM.exe	Get hash	malicious	Browse	
	Doc_43795379326436.PDF.exe	Get hash	malicious	Browse	
	aqa4dSbdFYw5DlK.exe	Get hash	malicious	Browse	
	IITuGuCnGifznoN.exe	Get hash	malicious	Browse	
	IITuGuCnGifznoN.exe	Get hash	malicious	Browse	
	RAHIM TRADING CO. FOR IMP.exe	Get hash	malicious	Browse	
	RAHIM TRADING CO. FOR IMP. & EXP.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
doc-file.ddns.net	PAYMENT-PO#987654567.exe	Get hash	malicious	Browse	• 194.5.97.7

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	PAYMENT-PO#987654567.exe	Get hash	malicious	Browse	• 194.5.97.7
	OUTSTANDING INVOICE.pdf.exe	Get hash	malicious	Browse	• 194.5.98.28
	Request Letter for Courtesy Call.xlsx	Get hash	malicious	Browse	• 194.5.97.61
	SecuriteInfo.com.Heur.23766.xls	Get hash	malicious	Browse	• 194.5.97.241
	SwiftCopy.pdf.exe	Get hash	malicious	Browse	• 194.5.98.31
	wlCqbMRJ7p.exe	Get hash	malicious	Browse	• 194.5.98.5
	SecuriteInfo.com.Trojan.PackedNET.832.3222.exe	Get hash	malicious	Browse	• 194.5.98.144
	SecuriteInfo.com.Trojan.PackedNET.831.12541.exe	Get hash	malicious	Browse	• 194.5.98.144
	0Cg1YYs1sv.exe	Get hash	malicious	Browse	• 194.5.98.144
	Duplicated Orders.xlsx	Get hash	malicious	Browse	• 194.5.98.144
	DEPOSITAR.xlsx	Get hash	malicious	Browse	• 194.5.98.144
	InvoicePOzGlybgcIc1vHasG.exe	Get hash	malicious	Browse	• 194.5.98.87
	POInvoiceOrderIuVvcl0VWEOAmXy.exe	Get hash	malicious	Browse	• 194.5.98.87
	payment invoice.exe	Get hash	malicious	Browse	• 194.5.98.23
	#RFQ ORDER484475577797.exe	Get hash	malicious	Browse	• 194.5.98.120
	b6yzWugw8V.exe	Get hash	malicious	Browse	• 194.5.98.107
	0041#Receipt.pif.exe	Get hash	malicious	Browse	• 194.5.98.180
	j07ghiByDq.exe	Get hash	malicious	Browse	• 194.5.97.146
	j07ghiByDq.exe	Get hash	malicious	Browse	• 194.5.97.146
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 194.5.97.18

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1438208
Entropy (8bit):	4.79869790235378
Encrypted:	false
SSDEEP:	12288:P6r9q+1i2mc3KEPdu4icYU/d+9x9/QV2HM5Jd+Zk3tsvON4Z1zOpz/YsQQyOTyMb:kKUw7Y1GOkqy0HPmH9pPQ4w5Q440X
MD5:	438425F009B373154E4E3629C3539581
SHA1:	5F686134A72FE1260D504DEDC88D8500C4F0C1F6
SHA-256:	B2262126A955E306DC68487333394DC08C4FBD708A19AFEB531F58916DDB1CFD
SHA-512:	7AE88A722C03871CF121708B026AE80D9A1B52AF52F6C42D908E4921B426C057C98ABFC0BB8AEEDBF761F9D709F80E9E0C5B96166A0A0B815DFC8DC376AD04A

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 41%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....B.....^.... .....@.. .....@..... ..@.....K.....4>..... ..... ..... ..H.....text...d.... ..... ..`.rsrc...4>.....@.....@..@.rel oc..... .....@..B.....@.....H.....PK.....%.....B...}.....}....*6.~8...(....&*z.(.....}.....}.....}....*B...}.....}....*..(.....}.....}.....}... ...}.....Z.s....}....*z.(.....}.....}.....} ...*..*R.(!.....s"...}#...*R.(!.....s'...}(...*>..} ....(.....*N.sA...}!....(!....*".(.....*".(.....*>..}#....(.....*N.sA...}'....(.....*>..}9....(.....*.r#..pr.a.p('...(K...(.. ...7...~M...~7...oR...oS.....8...*N.sA...}=....(8....*>..}N....(.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PAYMENT-PO#45678.exe.log	
Process:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	706
Entropy (8bit):	5.342604339328228
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21rkvoDLI4MWuCq1KDLI4Mq92n4M9XKbbDLI4MWuPJKiUrRZT:ML9E4Ks29E4Kx1qE4x84qXKDE4KhK3Vt
MD5:	9C1DF7CA80077C63698DCFE531754F1F
SHA1:	44E2DE975BF1364781A2E5EDE576D1FBCD948097
SHA-256:	78D4E6F15372E7DFE7C9D5C10BB515995A20AFAEF839C56E750CC336620BCFAB
SHA-512:	7078AFFB531F2AA5C813FB259C113CB1A02C992F76C47AAE036B8591C65EB4A2037B3BDAD83BBD4D30FA7D2CE244D9943C18EA8AA668FEBCD52B864E7476F8 4D
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken= b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=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..

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):	706
Entropy (8bit):	5.342604339328228
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21rkvoDLI4MWuCq1KDLI4Mq92n4M9XKbbDLI4MWuPJKiUrRZT:ML9E4Ks29E4Kx1qE4x84qXKDE4KhK3Vt
MD5:	9C1DF7CA80077C63698DCFE531754F1F
SHA1:	44E2DE975BF1364781A2E5EDE576D1FBCD948097
SHA-256:	78D4E6F15372E7DFE7C9D5C10BB515995A20AFAEF839C56E750CC336620BCFAB
SHA-512:	7078AFFB531F2AA5C813FB259C113CB1A02C992F76C47AAE036B8591C65EB4A2037B3BDAD83BBD4D30FA7D2CE244D9943C18EA8AA668FEBCD52B864E7476F8 4D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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..

C:\Users\user\AppData\Local\Temp\tmp8E26.tmp	
Process:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1306
Entropy (8bit):	5.143952376983823
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0/++xtn:cbk4oL600QydbQxIYODOLedq38Jj
MD5:	94EFA8AB0C786B66F62E9642A5B73D6D
SHA1:	3A8DB2E96347BCCBA05C6D471F0DB0A7A5C6D7BA
SHA-256:	2D6FC2F00387E055DD8D8F5D2CAD7116677E42DE42BF1970FEA67B5F975332F9
SHA-512:	B09DA0146DEB021868FA502CC6B728A6491147291FC5433AC2FE89B38A63DC7BCC1F438AD65632BEDBBF6DA8F12FBC5E1DD4359B06DCDF6FDD893FB4580C9F2
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp91A2.tmp	
Process:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe
File Type:	Non-ISO extended-ASCII text, with CR line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Pm:e
MD5:	0530B3218D0B896C1CD54343E50992B7
SHA1:	F9968CF5EC56B274F84643B360F66D3090F50DC8
SHA-256:	508C10049BB3DA3167A31B1A2C3A73B1686C145644070DB8A781D4CDE5C908C8
SHA-512:	744856560943FDCBE62881D2A55154DAD8CCDD2FC4D34CC89C9C5B8E25E4A60F20041E9C5BB200DC422B2273BC3979D39DC9A36676E5111B69CA4C5B299EF87
Malicious:	**true**
Preview:	...G1-.H

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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	43
Entropy (8bit):	4.85056969651225
Encrypted:	false
SSDEEP:	3:oNWXp5v1k+UdLAC:oNWXpFu+E0C
MD5:	FF0FB06F43AF0FC6F1463829F4A9482D
SHA1:	FA01AEC81BF55A5500363CF03FEB31206E1BAE12
SHA-256:	9AD4AEE3F7C04F11069D41167CFB9803790DC0E521560C57306DB97227A8C882
SHA-512:	D35314F2E04306256E30C5CB555C51B5D7B66EA0951511D87F469DBC462C607FCAA3191A52E60765CC086F276FF78ABFF9FFF4125C4D70ACA6A4E5BD48D83F7
Malicious:	false
Preview:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.79869790235378
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:	PAYMENT-PO#45678.exe
File size:	1438208
MD5:	438425f009b373154e4e3629c3539581
SHA1:	5f686134a72fe1260d504dedc88d8500c4f0c1f6
SHA256:	b2262126a955e306dc68487333394dc08c4fbd708a19afeb531f58916ddb1cfd
SHA512:	7ae88a722c03871cf121708b026ae80d9a1b52af52f6c42d908e4921b426c057c98abfc0bb8aeedbf761f9d709f80e9e0c5b96166a0a0b815dfc8dc376ad04aa
SSDEEP:	12288:P6r9q+1i2mc3KEPdu4icYU/d+9x9/QV2HM5Jd+Zk3tsvON4Z1zOpz/YsQQyOTyMb:kKUw7Y1GOkqy0HPmH9pPQ4w5Q440X
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....B.....^.... .....@.. .....@.....@.....

File Icon

Icon Hash:	81c0c1a14931c4c8

Static PE Info

General

Entrypoint:	0x52cd5e
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:	0x60B71CB7 [Wed Jun 2 05:52:55 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319

General

OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x12ad64	0x12ae00	False	0.478605480186	data	4.07686637612	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x12e000	0x33e34	0x34000	False	0.437903771034	data	5.71331335745	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x162000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 16:33:15.727742910 CEST	192.168.2.3	8.8.8.8	0xc76e	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:33:21.495158911 CEST	192.168.2.3	8.8.8.8	0x78d4	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:33:27.433357000 CEST	192.168.2.3	8.8.8.8	0x9ebb	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:33:48.615082979 CEST	192.168.2.3	8.8.8.8	0x50a9	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:33:54.439280987 CEST	192.168.2.3	8.8.8.8	0x69f1	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:00.090440035 CEST	192.168.2.3	8.8.8.8	0xb694	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:21.528187990 CEST	192.168.2.3	8.8.8.8	0x7e8e	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:27.071742058 CEST	192.168.2.3	8.8.8.8	0xbbf5	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:32.623429060 CEST	192.168.2.3	8.8.8.8	0x5029	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:53.377564907 CEST	192.168.2.3	8.8.8.8	0xac17	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:59.023550987 CEST	192.168.2.3	8.8.8.8	0xae58	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 16:35:04.499183893 CEST	192.168.2.3	8.8.8.8	0xc692	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)

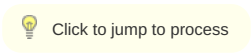
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 16:33:15.787997961 CEST	8.8.8.8	192.168.2.3	0xc76e	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:33:21.557796955 CEST	8.8.8.8	192.168.2.3	0x78d4	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:33:27.495415926 CEST	8.8.8.8	192.168.2.3	0x9ebb	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:33:48.675201893 CEST	8.8.8.8	192.168.2.3	0x50a9	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:33:54.489789009 CEST	8.8.8.8	192.168.2.3	0x69f1	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:00.152301073 CEST	8.8.8.8	192.168.2.3	0xb694	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:21.588874102 CEST	8.8.8.8	192.168.2.3	0x7e8e	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:27.132956982 CEST	8.8.8.8	192.168.2.3	0xbbf5	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:32.683567047 CEST	8.8.8.8	192.168.2.3	0x5029	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:53.436162949 CEST	8.8.8.8	192.168.2.3	0xac17	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:59.081986904 CEST	8.8.8.8	192.168.2.3	0xae58	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:04.557481050 CEST	8.8.8.8	192.168.2.3	0xc692	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PAYMENT-PO#45678.exe PID: 6600 Parent PID: 5800

General

Start time:	16:33:07
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PAYMENT-PO#45678.exe'
Imagebase:	0xd40000
File size:	1438208 bytes
MD5 hash:	438425F009B373154E4E3629C3539581
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: 00000000.00000002.208087031.00000000044CB000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.208087031.00000000044CB000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.208087031.00000000044CB000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.208570601.0000000004624000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.208570601.0000000004624000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.208570601.0000000004624000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.208595608.0000000004656000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.208595608.0000000004656000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.208595608.0000000004656000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: PAYMENT-PO#45678.exe PID: 6688 Parent PID: 6600

General

Start time:	16:33:08
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe
Imagebase:	0x70000
File size:	1438208 bytes
MD5 hash:	438425F009B373154E4E3629C3539581
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PAYMENT-PO#45678.exe PID: 6736 Parent PID: 6600

General

Start time:	16:33:09

Start date:	11/06/2021
Path:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe
Imagebase:	0x7d0000
File size:	1438208 bytes
MD5 hash:	438425F009B373154E4E3629C3539581
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: 00000003.00000000.203418579.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.203418579.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.203418579.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.473086416.0000000005440000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.473086416.0000000005440000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.203908472.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.203908472.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.203908472.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.473204133.0000000005540000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.473204133.0000000005540000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.473204133.0000000005540000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.468288291.0000000002E01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.471752842.0000000003E49000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.471752842.0000000003E49000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.464764845.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.464764845.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.464764845.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 6788 Parent PID: 6736

General

Start time:	16:33:12
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp8E26.tmp'
Imagebase:	0x1230000
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

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6800 Parent PID: 6788

General

Start time:	16:33:12
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: schtasks.exe PID: 6844 Parent PID: 6736

General

Start time:	16:33:13
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp91A2.tmp'
Imagebase:	0x1230000
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

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6860 Parent PID: 6844

General

Start time:	16:33:13
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: PAYMENT-PO#45678.exe PID: 6920 Parent PID: 528

General

Start time:	16:33:15
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe 0
Imagebase:	0x570000
File size:	1438208 bytes
MD5 hash:	438425F009B373154E4E3629C3539581
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: 00000008.00000002.225394409.0000000003E54000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.225394409.0000000003E54000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.225394409.0000000003E54000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.225464738.0000000003E86000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.225464738.0000000003E86000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.225464738.0000000003E86000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.224642029.0000000003CFB000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.224642029.0000000003CFB000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.224642029.0000000003CFB000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities — Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 6968 Parent PID: 528

General

Start time:	16:33:15
Start date:	11/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xd30000
File size:	1438208 bytes
MD5 hash:	438425F009B373154E4E3629C3539581
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: 00000009.00000002.227725816.0000000004646000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.227725816.0000000004646000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.227725816.0000000004646000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.227089559.00000000044BB000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.227089559.00000000044BB000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.227089559.00000000044BB000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.227679880.0000000004614000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.227679880.0000000004614000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.227679880.0000000004614000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 41%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: PAYMENT-PO#45678.exe PID: 7020 Parent PID: 6920

General

Start time:	16:33:16
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PAYMENT-PO#45678.exe
Imagebase:	0xde0000

File size:	1438208 bytes
MD5 hash:	438425F009B373154E4E3629C3539581
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: 0000000A.00000000.220271257.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.220271257.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.220271257.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.240713168.0000000004339000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.240713168.0000000004339000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.240622188.0000000003331000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.240622188.0000000003331000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.219525412.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.219525412.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.219525412.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.239124014.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.239124014.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.239124014.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: dhcpmon.exe PID: 7040 Parent PID: 6968

General

Start time:	16:33:17
Start date:	11/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x5b0000
File size:	1438208 bytes
MD5 hash:	438425F009B373154E4E3629C3539581
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: 0000000B.00000002.240871445.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.240871445.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.240871445.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.242717405.00000000029B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.242717405.00000000029B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.221925300.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.221925300.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.221925300.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.243007517.00000000039B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.243007517.00000000039B9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.221405279.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.221405279.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.221405279.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: dhcpmon.exe PID: 4952 Parent PID: 3388

General

Start time:	16:33:23
Start date:	11/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x1f0000
File size:	1438208 bytes
MD5 hash:	438425F009B373154E4E3629C3539581
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: 0000000C.00000002.242332686.0000000003A60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.242332686.0000000003A60000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.242332686.0000000003A60000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.241762181.000000000393B000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.241762181.000000000393B000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.241762181.000000000393B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: dhcpmon.exe PID: 6340 Parent PID: 4952

General

Start time:	16:33:25
Start date:	11/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x7b0000
File size:	1438208 bytes
MD5 hash:	438425F009B373154E4E3629C3539581
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: 0000000D.00000000.238827557.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.238827557.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.238827557.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.256058278.0000000002C71000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.256103684.0000000002CA8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000000.238326483.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.238326483.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.238326483.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.255169446.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.255169446.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.255169446.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.256151588.0000000003C79000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.256151588.0000000003C79000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Disassembly

Code Analysis