ID: 510055
Sample Name:
RHK098760045678009000.exe
Cookbook: default.jbs
Time: 12:34:11
Date: 27/10/2021
Version: 33.0.0 White Diamond

Table of Contents

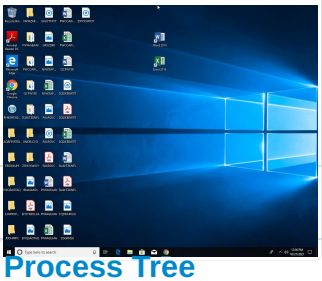
Windows Analysis Report RHK098760045678009000.exe

Overview

General Information

Sample Name:	RHK098760045678009000.exe
Analysis ID:	510055
MD5:	8ae8a20159a1fde.
SHA1:	a68c405aa1bec6..
SHA256:	bd386b60f5a095f..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

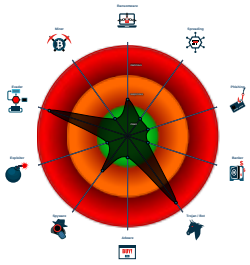
Nanocore

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Detected unpacking (overwrites its o…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Machine Learning detection for samp…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- RHK098760045678009000.exe (PID: 1744 cmdline: 'C:\Users\user\Desktop\RHK098760045678009000.exe' MD5: 8AE8A20159A1FDEDD8C4937E8CC4C571)
  - RHK098760045678009000.exe (PID: 4364 cmdline: 'C:\Users\user\Desktop\RHK098760045678009000.exe' MD5: 8AE8A20159A1FDEDD8C4937E8CC4C571)
    - schtasks.exe (PID: 2724 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpBEAC.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 2188 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - dhcpmon.exe (PID: 6216 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 8AE8A20159A1FDEDD8C4937E8CC4C571)
    - schtasks.exe (PID: 5728 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpC322.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RHK098760045678009000.exe (PID: 5820 cmdline: C:\Users\user\Desktop\RHK098760045678009000.exe 0 MD5: 8AE8A20159A1FDEDD8C4937E8CC4C571)
  - RHK098760045678009000.exe (PID: 2184 cmdline: C:\Users\user\Desktop\RHK098760045678009000.exe 0 MD5: 8AE8A20159A1FDEDD8C4937E8CC4C571)
- dhcpmon.exe (PID: 2724 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 8AE8A20159A1FDEDD8C4937E8CC4C571)
- dhcpmon.exe (PID: 6692 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 8AE8A20159A1FDEDD8C4937E8CC4C571)
  - dhcpmon.exe (PID: 6812 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 8AE8A20159A1FDEDD8C4937E8CC4C571)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "319d0527-f6c8-4b20-86a3-4c642aa0",
  "Group": "MONEY",
  "Domain1": "",
  "Domain2": "185.222.57.90",
  "Port": 4445,
  "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
00000017.00000001.311282865.000000000041 4000.00000040.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x111e5:$x1: NanoCore.ClientPluginHost • 0x11222:$x2: IClientNetworkHost • 0x14d55:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000017.00000001.311282865.000000000041 4000.00000040.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000017.00000001.311282865.000000000041 4000.00000040.00020000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x10f4d:$a: NanoCore • 0x10f5d:$a: NanoCore • 0x11191:$a: NanoCore • 0x111a5:$a: NanoCore • 0x111e5:$a: NanoCore • 0x10fac:$b: ClientPlugin • 0x111ae:$b: ClientPlugin • 0x111ee:$b: ClientPlugin • 0x110d3:$c: ProjectData • 0x11ada:$d: DESCrypto • 0x194a6:$e: KeepAlive • 0x17494:$g: LogClientMessage • 0x1368f:$i: get_Connected • 0x11e10:$j: #=q • 0x11e40:$j: #=q • 0x11e5c:$j: #=q • 0x11e8c:$j: #=q • 0x11ea8:$j: #=q • 0x11ec4:$j: #=q • 0x11ef4:$j: #=q • 0x11f10:$j: #=q

Source	Rule	Description	Author	Strings
0000000E.00000002.314320078.00000000038D 1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x123e5:$x1: NanoCore.ClientPluginHost • 0x7c6f3:$x1: NanoCore.ClientPluginHost • 0x8fe61:$x1: NanoCore.ClientPluginHost • 0xa8e25:$x1: NanoCore.ClientPluginHost • 0x12422:$x2: IClientNetworkHost • 0x7c70d:$x2: IClientNetworkHost • 0x8fe8e:$x2: IClientNetworkHost • 0xa8e52:$x2: IClientNetworkHost • 0x15f55:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000E.00000002.314320078.00000000038D 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 92 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.dhcpmon.exe.24f0000.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
14.2.dhcpmon.exe.24f0000.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
14.2.dhcpmon.exe.24f0000.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
14.2.dhcpmon.exe.24f0000.4.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:$j: #=q
0.2.RHK098760045678009000.exe.f051458.3. raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 118 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

.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:

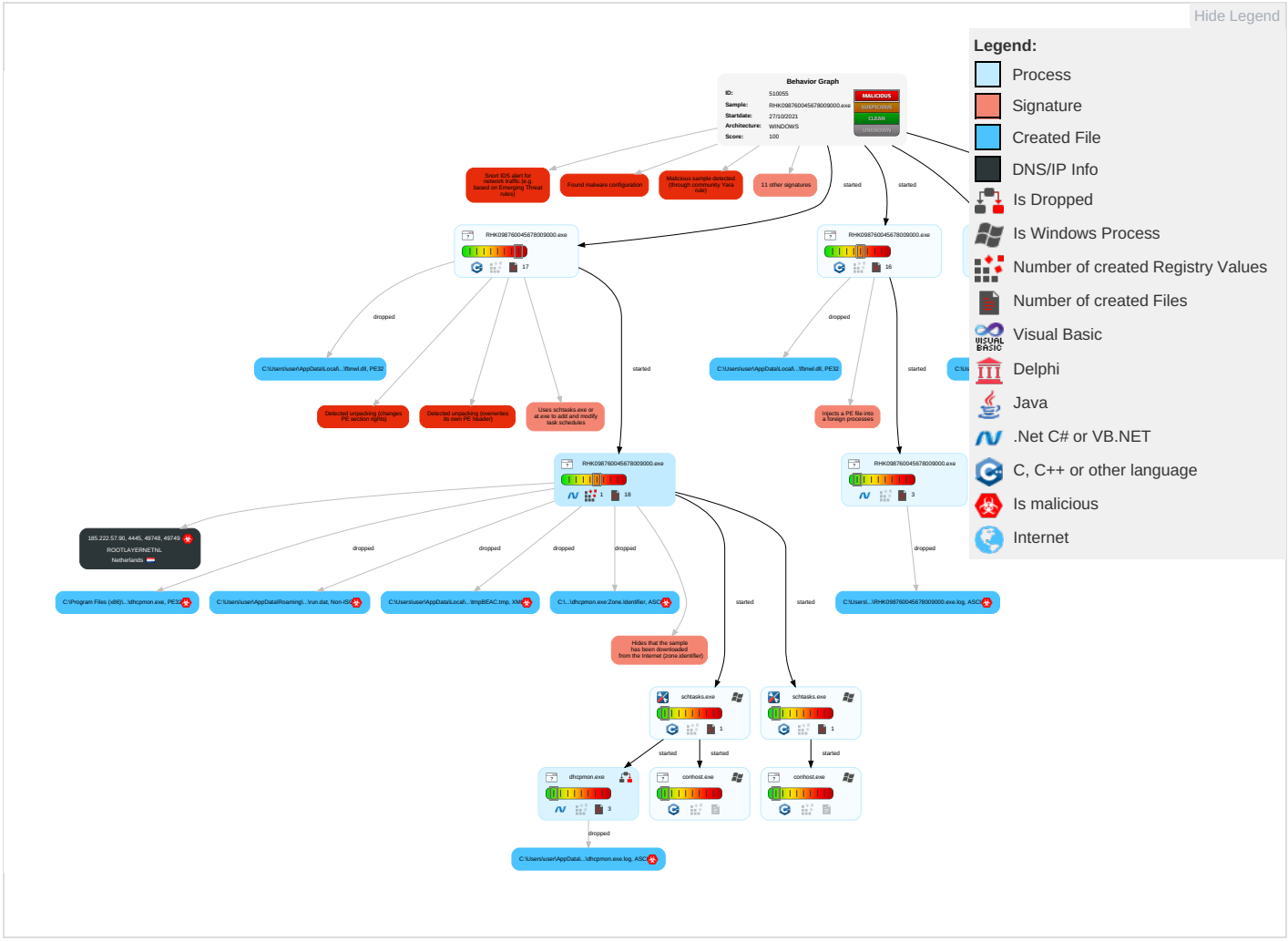
Detected Nanocore Rat

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
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 5	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Security Software Discovery 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

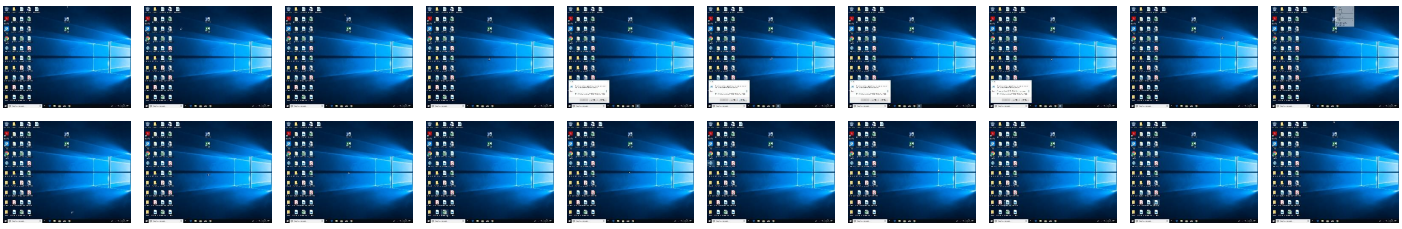
Behavior Graph



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
RHK098760045678009000.exe	29%	Virustotal		Browse
RHK098760045678009000.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	30%	ReversingLabs	Win32.Backdoor.Androm	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
23.0.dhcpmon.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
14.2.dhcpmon.exe.24f0000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.RHK098760045678009000.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
12.2.dhcpmon.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
14.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
23.2.dhcpmon.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.2.dhcpmon.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
14.0.dhcpmon.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.0.RHK098760045678009000.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Source	Detection	Scanner	Label	Link	Download
14.1.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.RHK0987600456780090000.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
12.0.dhcpmon.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
11.1.RHK0987600456780090000.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.RHK0987600456780090000.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
23.1.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.RHK0987600456780090000.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.0.RHK0987600456780090000.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
21.0.dhcpmon.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
11.2.RHK0987600456780090000.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.RHK0987600456780090000.exe.25f0000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
23.2.dhcpmon.exe.49a0000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
185.222.57.90	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
185.222.57.90	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.222.57.90	unknown	Netherlands		51447	ROOTLAYERNETNL	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510055
Start date:	27.10.2021
Start time:	12:34:11
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 11m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RHK098760045678009000.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@18/19@0/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 74.3% (good quality ratio 66.9%) • Quality average: 73.9% • Quality standard deviation: 33.3%
HCA Information:	• Successful, ratio: 83% • 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
12:35:20	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\RHK098760045678009000.exe" s>$(Arg0)
12:35:21	API Interceptor	916x Sleep call for process: RHK098760045678009000.exe modified
12:35:23	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
12:35:23	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.222.57.90	FHKPO098765432345.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ROOTLAYERNETNL	FHKPO098765432345.exe	Get hash	malicious	Browse	• 185.222.57.90
	SecuriteInfo.com.Suspicious.Win32.Save.a.4240.exe	Get hash	malicious	Browse	• 185.222.58.151
	SecuriteInfo.com.Artemis3008D0721A6C.1070.exe	Get hash	malicious	Browse	• 185.222.58.151
	AWB #3099657260.xlsx	Get hash	malicious	Browse	• 185.222.57.190

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HIC INTERNATIONAL - REQUEST FOR QUOTATION DOCUMENTS.exe	Get hash	malicious	Browse	• 45.137.22.70
	AWB #30996572600.xlsx	Get hash	malicious	Browse	• 185.222.57.190
	BL. NO. ANSMUNDAR3621.exe	Get hash	malicious	Browse	• 185.222.57.71
	Payment Supplier.xlsx	Get hash	malicious	Browse	• 185.222.57.85
	BULK ORDER #RFQ REF R2100131410.exe	Get hash	malicious	Browse	• 45.137.22.70
	Proforma Invoices.exe	Get hash	malicious	Browse	• 45.137.22.77
	TT copy.exe	Get hash	malicious	Browse	• 185.222.57.71
	EXT-Order-ES.xlsx	Get hash	malicious	Browse	• 185.222.57.190
	attached MT103.xlsx	Get hash	malicious	Browse	• 185.222.57.85
	invoice.exe	Get hash	malicious	Browse	• 185.222.57.71
	pHflio3D4E.exe	Get hash	malicious	Browse	• 45.137.22.77
	Kyodo International Corp - Products Lists.exe	Get hash	malicious	Browse	• 185.222.57.253
	tgSQwVSEzE.exe	Get hash	malicious	Browse	• 45.137.22.77
	Keen-Pros-DOC310521-31052021124021.exe	Get hash	malicious	Browse	• 45.137.22.70
	Order EQE090.xlsx	Get hash	malicious	Browse	• 185.222.57.190
	PO-10152021.exe	Get hash	malicious	Browse	• 185.222.58.151

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\RHK0987600456780090000.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	446374
Entropy (8bit):	7.37562465733928
Encrypted:	false
SSDEEP:	6144:vBlL/qJ0hAJgtOHh6K6wiqyv/9nWZbcqzr2VURH2W1yS1dk3kqA/eFaTQH:J+0hAgtOHEK61B/9yn662WwS1dkdAfTo
MD5:	8AE8A20159A1FDEDD8C4937E8CC4C571
SHA1:	A68C405AA1BEC64C9790C321B4785C98F5C9A2A6
SHA-256:	BD386B60F5A095F369D4473D5F3185C226363A563F45326CEA048E10F0FF403B
SHA-512:	AE7EC190DB374595C4612F937F8FF98172B4A9C828E218806498E6443C0490CFDF92FE7A8F2B965DC34015C5B5E004DD02C53289A55C94E194F079B0E8017261
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....;.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc....;.....<...x.....@..@..... ....

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

Process:	C:\Users\user\Desktop\RHK0987600456780090000.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

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RHK098760045678009000.exe.log	
Process:	C:\Users\user\Desktop\RHK098760045678009000.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_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\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
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\Local\Temp\9re2jblvico	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	data
Category:	dropped
Size (bytes):	279039
Entropy (8bit):	7.9862471646957305
Encrypted:	false
SSDEEP:	6144:05TTwU+xMf7+UF1tCr0XpS6i/qpwSu47UNIp9U7iWwK:+TyxMD+UF/CEpTsYwSu2QItK
MD5:	EF5501D8A05A00E32A4DA2E879054CAB
SHA1:	EE96AF9CAA8A0B968D5664A61CAEF4A18C7F097F
SHA-256:	60C2C9E683635BC40FCBC61E06A25532D00E6BA4D46624C7C57E71580AE84DCF
SHA-512:	D636286954326E505FC524A21B8D1540AD1F66A84C513B87BA9027D12C4A3EF74F14D0707AE5E88F8432DBCE3A7ABB98D61DEFA7B740E4CF3342C0463874E8F
Malicious:	false
Preview:	9c..\)..... .".\a2).H<....i>..z..T%.b...=i.q..).k.....Am..[c.Z.%...p[$W.n.a-..../E....\|8.p..vY..1.....)Z.,-u/....j.....{.@....:...U.A..L.%...B...../"u.#..p.. ..]/n!.....~...W...du.X..!Jh}.....q$..x..v..0.|..ed...~,:.r.....8"j.....V.....5....)..... k.7\.t[.H<..c.i>..p.4..b:..=..q..).;...6Am.`[c.#.I...p.....x.[fZ.=h...x..Ea...A..}...a!..%x....L..PK,....\.{..|...o^.....|O.+E$..jx..HV...P..Pd.2.I#.!:.[....J{..~T..v.F.k.*..K...../bk.).!O...X8...U.T]lxr.i.....b....p..V.....v,.ZL).... I..\`.).H...c.i>..z..T%.....Y.)h.).....\Am..[c.AZ.IA..pX....K..[nd..R_..x^.&a...A..}...H...:x....L...^,...A3.{.w\|....5..5..C.6..8.O...$..jx.H...*...P..c.I..!Y..m'.J{..~T..v.F.k.*.|.K.....!O...X8...UwT]w3r.i.....b....p..V.....5....)..'.. I1.\`2).H<..c.i>..z..T%.b...=i.q..).k.....Am..[c.Z.IA..pX....K.x.[f..]h...x..&a...A..}...a...:x....L...P.,.....{..|...o^.....C....8.O...$..jx..HV...P..Pd.2.I#.!Y...m..J{..~T..v.F.k.*..K.....!O...X8...UwT]w3r.

C:\Users\user\AppData\Local\Temp\nsf6352.tmp\fbnwl.dll	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	modified

C:\Users\user\AppData\Local\Temp\nsf6352.tmp\fbnwl.dll	
Size (bytes):	22016
Entropy (8bit):	6.644684115150565
Encrypted:	false
SSDEEP:	384:4sowZo58r1ZAbGTBDPHglPB51T7nkxop4D+Znha2+K5wUcatJsIfX:Cwu58r1oGTBGPK6pq+p42+ZCtJsA
MD5:	1288423DC0799D420E65125515BA8198
SHA1:	F1CB23453DFEFED3BD256EBD8FE9C1FCE230E901
SHA-256:	BE749029D5FFBA43EBCD1BE38E8486BA88FD77A39B08266CFE79C9FA21CF3466
SHA-512:	60B548402CC56A944EAF8BBE0186F02633BED0F267154BEA5844273C13F4B122D2EA7D8980B288AA0D272A742D49107E6DE558B26BDD98583F787AC7D1895BA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... T._A:._A:._A:.....^A:..^>.]A:..]4.^A:..^0.[A:.K*;.JA:._A;..A:...>.^A:. ..:.^A:.....^A:...8.^A:.Rich_A:.....PE..L.....ya.....!.....&...,.....@.....@.....A..L...xC.....p.....A..... .....@..p.....text..."$.....&..... ..`.rdata.....@.....*.....@..@.data.....P.....6.....@....rsrc.....p.....P.....@..@.reloc.....R .....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsr3472.tmp\fbnwl.dll	
Process:	C:\Users\user\Desktop\RHK098760045678009000.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	22016
Entropy (8bit):	6.644684115150565
Encrypted:	false
SSDEEP:	384:4sowZo58r1ZAbGTBDPHglPB51T7nkxop4D+Znha2+K5wUcatJsIfX:Cwu58r1oGTBGPK6pq+p42+ZCtJsA
MD5:	1288423DC0799D420E65125515BA8198
SHA1:	F1CB23453DFEFED3BD256EBD8FE9C1FCE230E901
SHA-256:	BE749029D5FFBA43EBCD1BE38E8486BA88FD77A39B08266CFE79C9FA21CF3466
SHA-512:	60B548402CC56A944EAF8BBE0186F02633BED0F267154BEA5844273C13F4B122D2EA7D8980B288AA0D272A742D49107E6DE558B26BDD98583F787AC7D1895BA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... T._A:._A:._A:.....^A:..^>.]A:..]4.^A:..^0.[A:.K*;.JA:._A;..A:...>.^A:. ..:.^A:.....^A:...8.^A:.Rich_A:.....PE..L.....ya.....!.....&...,.....@.....@.....A..L...xC.....p.....A..... .....@..p.....text..."$.....&..... ..`.rdata.....@.....*.....@..@.data.....P.....6.....@....rsrc.....p.....P.....@..@.reloc.....R .....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsv5920.tmp\fbnwl.dll	
Process:	C:\Users\user\Desktop\RHK098760045678009000.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	22016
Entropy (8bit):	6.644684115150565
Encrypted:	false
SSDEEP:	384:4sowZo58r1ZAbGTBDPHglPB51T7nkxop4D+Znha2+K5wUcatJsIfX:Cwu58r1oGTBGPK6pq+p42+ZCtJsA
MD5:	1288423DC0799D420E65125515BA8198
SHA1:	F1CB23453DFEFED3BD256EBD8FE9C1FCE230E901
SHA-256:	BE749029D5FFBA43EBCD1BE38E8486BA88FD77A39B08266CFE79C9FA21CF3466
SHA-512:	60B548402CC56A944EAF8BBE0186F02633BED0F267154BEA5844273C13F4B122D2EA7D8980B288AA0D272A742D49107E6DE558B26BDD98583F787AC7D1895BA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... T._A:._A:._A:.....^A:..^>.]A:..]4.^A:..^0.[A:.K*;.JA:._A;..A:...>.^A:. ..:.^A:.....^A:...8.^A:.Rich_A:.....PE..L.....ya.....!.....&...,.....@.....@.....A..L...xC.....p.....A..... .....@..p.....text..."$.....&..... ..`.rdata.....@.....*.....@..@.data.....P.....6.....@....rsrc.....p.....P.....@..@.reloc.....R .....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsv8A14.tmp\fbnwl.dll	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	22016
Entropy (8bit):	6.644684115150565
Encrypted:	false
SSDEEP:	384:4sowZo58r1ZAbGTBDPHglPB51T7nkxop4D+Znha2+K5wUcatJsIfX:Cwu58r1oGTBGPK6pq+p42+ZCtJsA
MD5:	1288423DC0799D420E65125515BA8198
SHA1:	F1CB23453DFEFED3BD256EBD8FE9C1FCE230E901
SHA-256:	BE749029D5FFBA43EBCD1BE38E8486BA88FD77A39B08266CFE79C9FA21CF3466
SHA-512:	60B548402CC56A944EAF8BBE0186F02633BED0F267154BEA5844273C13F4B122D2EA7D8980B288AA0D272A742D49107E6DE558B26BDD98583F787AC7D1895BA
Malicious:	false

C:\Users\user\AppData\Local\Temp\nsv8A14.tmp\fbnwl.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... T._A:._A:._A:.....^A:..^>.]A:..]4.^A:..^0.[A:.K*;.JA:._A;..A:...>.^A:. ..:.^A:.....^A:...8.^A:.Rich_A:.....PE..L.....ya.....!.....&.....@.....@.....A..L...xC.....p.....A..... .....@..p.....text..."$.....&..... ..`.rdata.....@.....*.....@..@.data.....P.....6.....@....rsrc.....p.....P.....@..@.reloc.....R .....@..B..... .....

C:\Users\user\AppData\Local\Temp\tmpBEAC.tmp	
Process:	C:\Users\user\Desktop\RHK098760045678009000.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1315
Entropy (8bit):	5.148995150358009
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK07bxtn:cbk4oL600QydbQxIYODOLedq3Wj
MD5:	EA990AF5897960534A4B53B9AE469852
SHA1:	C9409D6DA2EF73DA46D2F252FACDA1577F7B31C8
SHA-256:	16415204477AB850AF7AA39E29ADD5D6BB0DA97F2E8BB68F906D3B82F9BEE163
SHA-512:	DAA2BDEB5CA246B5D7383005FE2A4B3975321B4330E8777AD71FDD840A057F17E12137FBDC3FFB86346C23A755BC230E2ECABD68BBCC215D11EA506A684A46 A4
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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\RHK098760045678009000.exe
File Type:	data
Category:	modified
Size (bytes):	232
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKgmR7kkmefoeLBizbCuVkqYM:X4LDAnybgCFcps0OafmCYDlizZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005
SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF385 1
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+ .2e'..E?.G.....[.&

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\RHK098760045678009000.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:HCf:if
MD5:	AB6ACF2514CF9D7C146288805B82395A
SHA1:	B45A987160D4F1CF2BF65398D7BDB0DDFDF966F9
SHA-256:	4ADBC5F80F47F6FC3B6EF126648722F05DE66E8F32A6248B08AEB3F986B99D76
SHA-512:	6F93CE445AB368DC3DAC4A81C3814AB8F0DD2E8C5CA67532C1171E676BA792F5101DBE25A587198FA75130C0DCF309460DDD1E50AE46FDE55141B0820FB49B F
Malicious:	**true**
Preview:	s....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\Desktop\RHK098760045678009000.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Size (bytes):	24
Entropy (8bit):	4.584962500721156
Encrypted:	false
SSDEEP:	3:9bzY6oRDJoTBn:RzWDqTB
MD5:	3FCC766D28BFD974C68B38C27D0D7A9A
SHA1:	45ED19A78D9B79E46EDBFC3E3CA58E90423A676B
SHA-256:	39A25F1AB5099005A74CF04F3C61C3253CD9BDA73B85228B58B45AAA4E838641
SHA-512:	C7D47BDAABEEBB8C9D9B31CC4CE968EAF291771762FA022A2F55F9BA4838E71FDBD3F83792709E47509C5D94629D6D274CC933371DC01560D13016D944012D 5
Malicious:	false
Preview:	9iH...}Z.4..f.....l.d

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\RHK098760045678009000.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44 F8
Malicious:	false
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\RHK098760045678009000.exe
File Type:	data
Category:	dropped
Size (bytes):	426832
Entropy (8bit):	**7.999527918131335**
Encrypted:	**true**
SSDEEP:	6144:zKfHbamD8WN+JQYrjM7Ei2CsFJjyh9zvgPonV5HqZcPVT4Eb+Z6no3QSzjeMsdF/:zKf137EiDsTjevgArYcPVLoTQS+0iv
MD5:	653DDDCB6C89F6EC51F3DDC0053C5914
SHA1:	4CF7E7D42495CE01C261E4C5C4B8BF6CD76CCEE5
SHA-256:	83B9CAE66800C768887FB270728F6806CBEBDEAD9946FA730F01723847F17FF9
SHA-512:	27A467F2364C21CD1C6C34EF1CA5FFB09B4C3180FC9C025E293374EB807E4382108617BB4B97F8EBBC27581CD6E5988BB5E21276B3CB829C1C0E49A6FC9463A
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^.._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m. ..RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:...L.g<.....I..%4[.G^.~.I'.....v .p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`'].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44 Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...."..bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&... .g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\RHK098760045678009000.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	52
Entropy (8bit):	4.4002543244019225
Encrypted:	false
SSDEEP:	3:oN0naRR3c2dSTuCU/Ln:oNcSRlQTSTn
MD5:	6E6E1881C289567E83AAD0435BF4C72D
SHA1:	29DB6951579EA2E838154DED33E575806C797AA7
SHA-256:	3956537EFB18EC09EA2D6A0B831DBFC9EACFE59364873C8D5B55F8C21BCF46C3
SHA-512:	62D095D1DCD6184799D3E26F6473F39037C4804D1400844E347EA30AEF12B4667C141FC2A9F184F8C7C2CE852E4B154B1600DE5C338E4BA6710EBD9E1FDBCC2
Malicious:	false
Preview:	C:\Users\user\Desktop\RHK098760045678009000.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.37562465733928
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	RHK098760045678009000.exe
File size:	446374
MD5:	8ae8a20159a1fdedd8c4937e8cc4c571
SHA1:	a68c405aa1bec64c9790c321b4785c98f5c9a2a6
SHA256:	bd386b60f5a095f369d4473d5f3185c226363a563f45326cea048e10f0ff403b
SHA512:	ae7ec190db374595c4612f937f8ff98172b4a9c828e218806498e6443c0490cfdf92fe7a8f2b965dc34015c5b5e004dd02c53289a55c94e194f079b0e8017261
SSDEEP:	6144:vBlL/qJ0hAJgtOHh6K6wiqyv/9nWZbcqzr2VURH2W1yS1dk3kqA/eFaTQH:J+0hAgtOHEK61B/9yn662WwS1dkdAfTo
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF..rv..QF..W@..QF.Rich.QF.....PE..L...e:.V.....\.....0.....p....@

File Icon

Icon Hash:	30f0ccbaf2e47182

Static PE Info

General

Entrypoint:	0x4030fb
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x56FF3A65 [Sat Apr 2 03:20:05 2016 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:	b76363e9cb88bf9390860da8e50999d2

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5aeb	0x5c00	False	0.665123980978	data	6.42230569414	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x7000	0x1196	0x1200	False	0.458984375	data	5.20291736659	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1b038	0x600	False	0.432291666667	data	4.0475118296	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2d000	0x23b90	0x23c00	False	0.522324355332	data	5.54550086743	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/27/21-12:35:22.661932	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	4445	192.168.2.7	185.222.57.90
10/27/21-12:35:30.385238	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49749	4445	192.168.2.7	185.222.57.90
10/27/21-12:35:36.308156	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	4445	192.168.2.7	185.222.57.90
10/27/21-12:35:42.259470	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	4445	192.168.2.7	185.222.57.90
10/27/21-12:35:46.512767	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	4445	192.168.2.7	185.222.57.90
10/27/21-12:35:52.967208	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	4445	192.168.2.7	185.222.57.90
10/27/21-12:35:59.180187	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	4445	192.168.2.7	185.222.57.90
10/27/21-12:36:06.219324	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	4445	192.168.2.7	185.222.57.90
10/27/21-12:36:12.240861	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	4445	192.168.2.7	185.222.57.90
10/27/21-12:36:18.449942	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49787	4445	192.168.2.7	185.222.57.90
10/27/21-12:36:25.461735	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49803	4445	192.168.2.7	185.222.57.90
10/27/21-12:36:31.504021	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49807	4445	192.168.2.7	185.222.57.90
10/27/21-12:36:37.609565	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49808	4445	192.168.2.7	185.222.57.90
10/27/21-12:36:42.275628	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49817	4445	192.168.2.7	185.222.57.90
10/27/21-12:36:49.658333	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49834	4445	192.168.2.7	185.222.57.90
10/27/21-12:36:55.470444	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49835	4445	192.168.2.7	185.222.57.90
10/27/21-12:37:01.316047	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49836	4445	192.168.2.7	185.222.57.90
10/27/21-12:37:07.236455	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49841	4445	192.168.2.7	185.222.57.90
10/27/21-12:37:13.129562	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49842	4445	192.168.2.7	185.222.57.90
10/27/21-12:37:19.018469	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49843	4445	192.168.2.7	185.222.57.90

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: RHK098760045678009000.exe PID: 1744 Parent PID: 6048

General

Start time:	12:35:11
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\RHK098760045678009000.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RHK098760045678009000.exe'
Imagebase:	0x400000
File size:	446374 bytes
MD5 hash:	8AE8A20159A1FDEDD8C4937E8CC4C571
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.265580508.000000000F040000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.265580508.000000000F040000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.265580508.000000000F040000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.265580508.000000000F040000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: RHK098760045678009000.exe PID: 4364 Parent PID: 1744

General

Start time:	12:35:12
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\RHK098760045678009000.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RHK098760045678009000.exe'
Imagebase:	0x400000
File size:	446374 bytes
MD5 hash:	8AE8A20159A1FDEDD8C4937E8CC4C571
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.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: 2724 Parent PID: 4364

General

Start time:	12:35:19
Start date:	27/10/2021
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\tmpBEAC.tmp'
Imagebase:	0x10b0000
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: 2188 Parent PID: 2724

General

Start time:	12:35:20
Start date:	27/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: RHK098760045678009000.exe PID: 5820 Parent PID: 1104

General

Start time:	12:35:20
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\RHK098760045678009000.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\RHK098760045678009000.exe 0
Imagebase:	0x11a0000
File size:	446374 bytes
MD5 hash:	8AE8A20159A1FDEDD8C4937E8CC4C571
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.292543029.000000000F030000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.292543029.000000000F030000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.292543029.000000000F030000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.292543029.000000000F030000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5728 Parent PID: 4364

General

Start time:	12:35:20
Start date:	27/10/2021
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\tmpC322.tmp'
Imagebase:	0x10b0000
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: 1388 Parent PID: 5728

General

Start time:	12:35:21
Start date:	27/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: RHK098760045678009000.exe PID: 2184 Parent PID: 5820

General

Start time:	12:35:22
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\RHK098760045678009000.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\RHK098760045678009000.exe 0
Imagebase:	0x400000
File size:	446374 bytes
MD5 hash:	8AE8A20159A1FDEDD8C4937E8CC4C571
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.306617686.0000000002A3E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.304923421.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.304923421.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.304923421.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.304923421.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000001.289620419.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000001.289620419.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000001.289620419.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.306384984.00000000025F2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.306384984.00000000025F2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.306384984.00000000025F2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.306683045.0000000003A31000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.306683045.0000000003A31000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.306683045.0000000003A31000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.305718280.0000000000615000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.305718280.0000000000615000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.305718280.0000000000615000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.306281947.0000000002490000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.306281947.0000000002490000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.306281947.0000000002490000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.306281947.0000000002490000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 2724 Parent PID: 1104

General

Start time:	12:35:23
Start date:	27/10/2021

Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x400000
File size:	446374 bytes
MD5 hash:	8AE8A20159A1FDEDD8C4937E8CC4C571
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.300740057.000000000F050000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.300740057.000000000F050000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.300740057.000000000F050000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.300740057.000000000F050000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 30%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: dhcpmon.exe PID: 6216 Parent PID: 2724

General

Start time:	12:35:25
Start date:	27/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x400000
File size:	446374 bytes
MD5 hash:	8AE8A20159A1FDEDD8C4937E8CC4C571
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.314320078.00000000038D1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.314320078.00000000038D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.314320078.00000000038D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000001.298075260.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000001.298075260.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000001.298075260.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.313620230.0000000000715000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.313620230.0000000000715000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.313620230.0000000000715000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.313348558.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.313348558.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.313348558.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.313348558.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.314060593.00000000024F2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.314060593.00000000024F2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.314060593.00000000024F2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.313999047.00000000024A0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.313999047.00000000024A0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.313999047.00000000024A0000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.313999047.00000000024A0000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.314285351.00000000028DE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 6692 Parent PID: 3292

General

Start time:	12:35:33

Start date:	27/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x400000
File size:	446374 bytes
MD5 hash:	8AE8A20159A1FDEDD8C4937E8CC4C571
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.314003400.000000000F050000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.314003400.000000000F050000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.314003400.000000000F050000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.314003400.000000000F050000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: dhcpmon.exe PID: 6812 Parent PID: 6692

General

Start time:	12:35:34
Start date:	27/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x400000
File size:	446374 bytes
MD5 hash:	8AE8A20159A1FDEDD8C4937E8CC4C571
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: 00000017.00000001.311282865.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000001.311282865.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000001.311282865.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.327568976.000000000282E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000002.327700810.0000000004960000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000017.00000002.327700810.0000000004960000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.327700810.0000000004960000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.327700810.0000000004960000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000002.327748596.00000000049A2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.327748596.00000000049A2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.327748596.00000000049A2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000002.327015327.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000017.00000002.327015327.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.327015327.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.327015327.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000002.327148918.00000000004B5000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.327148918.00000000004B5000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.327148918.00000000004B5000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000002.327594984.0000000003821000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.327594984.0000000003821000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.327594984.0000000003821000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis