ID: 384149
Sample Name:
bGf2H3tXGg.exe
Cookbook: default.jbs
Time: 17:20:12
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

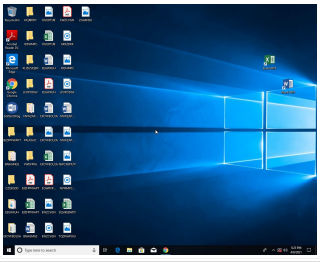
Analysis Report bGf2H3tXGg.exe

Overview

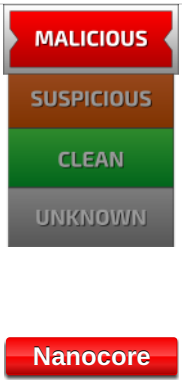
General Information

Sample Name:	bGf2H3tXGg.exe
Analysis ID:	384149
MD5:	f72a7fd231e50f9…
SHA1:	1ac9f0876ec8f4b..
SHA256:	fb01157b437b00f..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



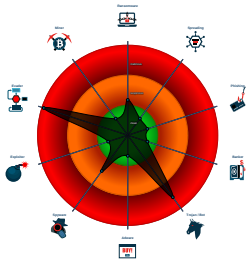
Nanocore

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

Signatures

- Antivirus detection for dropped file
- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- Detected unpacking (creates a PE fi…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Contains functionality to prevent loa…

Classification



Startup

- **System is w10x64**
- bGf2H3tXGg.exe (PID: 4656 cmdline: 'C:\Users\user\Desktop\bGf2H3tXGg.exe' MD5: F72A7FD231E50F9B43C3DAB470364846)
  - bGf2H3tXGg.exe (PID: 204 cmdline: 'C:\Users\user\Desktop\bGf2H3tXGg.exe' MD5: F72A7FD231E50F9B43C3DAB470364846)
    - schtasks.exe (PID: 6280 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpDE28.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6288 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6320 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpE0E8.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6456 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- bGf2H3tXGg.exe (PID: 6468 cmdline: C:\Users\user\Desktop\bGf2H3tXGg.exe 0 MD5: F72A7FD231E50F9B43C3DAB470364846)
  - bGf2H3tXGg.exe (PID: 6704 cmdline: C:\Users\user\Desktop\bGf2H3tXGg.exe 0 MD5: F72A7FD231E50F9B43C3DAB470364846)
- dhcpmon.exe (PID: 6600 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: F72A7FD231E50F9B43C3DAB470364846)
  - dhcpmon.exe (PID: 6816 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: F72A7FD231E50F9B43C3DAB470364846)
- dhcpmon.exe (PID: 6752 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: F72A7FD231E50F9B43C3DAB470364846)
  - dhcpmon.exe (PID: 6212 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: F72A7FD231E50F9B43C3DAB470364846)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "ccf3c62d-d356-4a80-bb94-307bc35a",
  "Group": "Backup",
  "Domain1": "backu4734.duckdns.org",
  "Domain2": "backu4734.duckdns.org",
  "Port": 8092,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "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
00000003.00000002.494409950.0000000004E7 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000003.00000002.494409950.0000000004E7 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000003.00000002.494409950.0000000004E7 2000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
0000000E.00000002.318797223.00000000034E 1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x146bd:$x1: NanoCore.ClientPluginHost • 0x146fa:$x2: IClientNetworkHost • 0x1822d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000E.00000002.318797223.00000000034E 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 125 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
22.2.dhcpmon.exe.24bcc88.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
22.2.dhcpmon.exe.24bcc88.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
11.2.bGf2H3tXGg.exe.29c1458.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
11.2.bGf2H3tXGg.exe.29c1458.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
11.2.bGf2H3tXGg.exe.29c1458.3.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 355 entries				

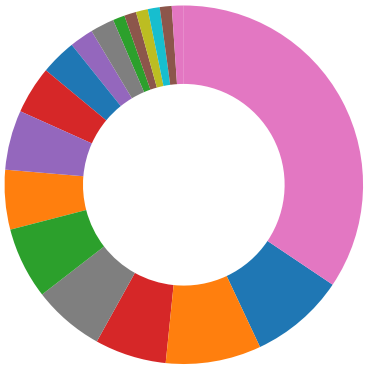
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file

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

Compliance:

Detected unpacking (creates a PE file in dynamic memory)

Detected unpacking (overwrites its own PE header)

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (creates a PE file in dynamic memory)

Detected unpacking (overwrites its own PE header)

.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:

Contains functionality to prevent local Windows debugging

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

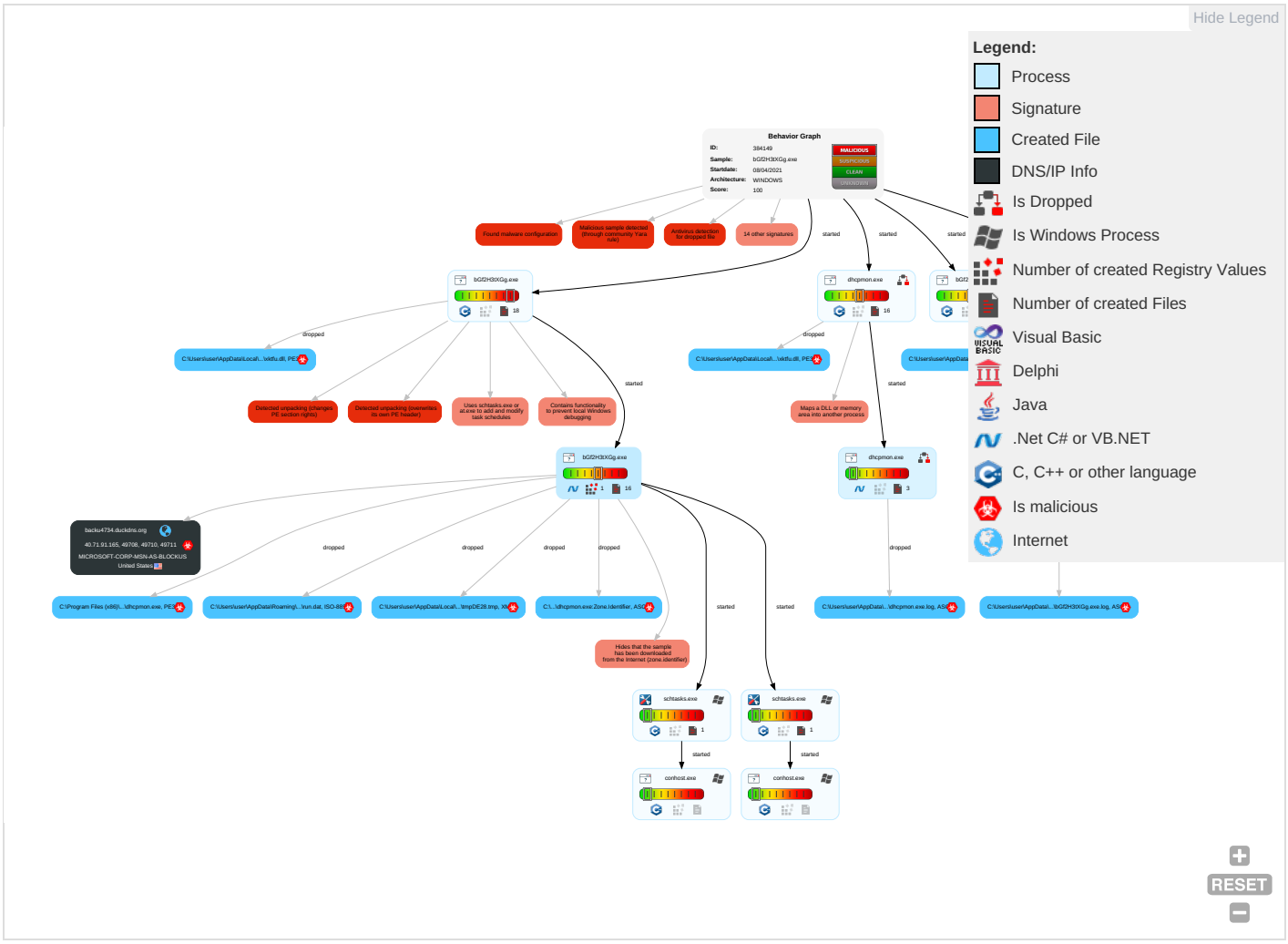
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control

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	Access Token Manipulation 1	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	Process Injection 2 1 2	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)	Scheduled Task/Job 1	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 2 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 4 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Security Software Discovery 1 4	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3 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	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 3 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	Process Injection 2 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

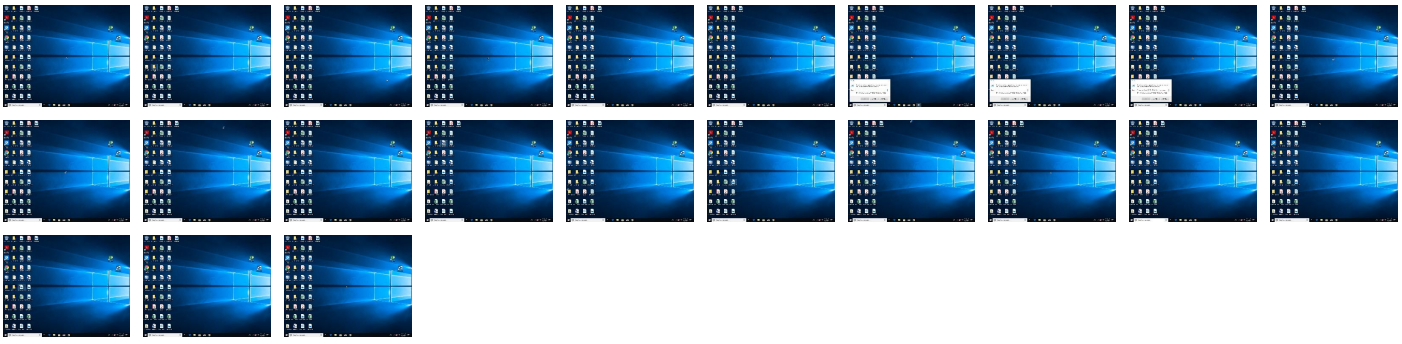
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
bGf2H3tXGg.exe	51%	Virustotal		Browse
bGf2H3tXGg.exe	16%	Metadefender		Browse
bGf2H3tXGg.exe	69%	ReversingLabs	Win32.Trojan.Zenpak	
bGf2H3tXGg.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsfEFEC.tmp\xktfu.dll	100%	Avira	HEUR/AGEN.1120893	
C:\Users\user\AppData\Local\Temp\nsh9AB8.tmp\xktfu.dll	100%	Avira	HEUR/AGEN.1120893	
C:\Users\user\AppData\Local\Temp\nsmE619.tmp\xktfu.dll	100%	Avira	HEUR/AGEN.1120893	
C:\Users\user\AppData\Local\Temp\nsp1382.tmp\xktfu.dll	100%	Avira	HEUR/AGEN.1120893	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	51%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	16%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	69%	ReversingLabs	Win32.Trojan.Zenpak	
C:\Users\user\AppData\Local\Temp\nsfEFEC.tmp\xktfu.dll	19%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsfEFEC.tmp\xktfu.dll	14%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsfEFEC.tmp\xktfu.dll	41%	ReversingLabs	Win32.Trojan.InjectorX	
C:\Users\user\AppData\Local\Temp\nsh9AB8.tmp\xktfu.dll	19%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsh9AB8.tmp\xktfu.dll	14%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsh9AB8.tmp\xktfu.dll	41%	ReversingLabs	Win32.Trojan.InjectorX	
C:\Users\user\AppData\Local\Temp\nsmE619.tmp\xktfu.dll	19%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsmE619.tmp\xktfu.dll	14%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsmE619.tmp\xktfu.dll	41%	ReversingLabs	Win32.Trojan.InjectorX	
C:\Users\user\AppData\Local\Temp\nsp1382.tmp\xktfu.dll	19%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsp1382.tmp\xktfu.dll	14%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsp1382.tmp\xktfu.dll	41%	ReversingLabs	Win32.Trojan.InjectorX	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.bGf2H3tXGg.exe.4e70000.16.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
22.2.dhcpmon.exe.2430000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.0.bGf2H3tXGg.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
22.1.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.2.dhcpmon.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
15.2.dhcpmon.exe.10000000.5.unpack	100%	Avira	HEUR/AGEN.1120893		Download File
14.1.bGf2H3tXGg.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.2.bGf2H3tXGg.exe.4a80000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.dhcpmon.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
22.2.dhcpmon.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.bGf2H3tXGg.exe.10000000.5.unpack	100%	Avira	HEUR/AGEN.1120893		Download File
11.2.bGf2H3tXGg.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
11.0.bGf2H3tXGg.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
17.0.dhcpmon.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
22.0.dhcpmon.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.2.bGf2H3tXGg.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
12.2.dhcpmon.exe.10000000.5.unpack	100%	Avira	HEUR/AGEN.1120893		Download File
14.2.bGf2H3tXGg.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.bGf2H3tXGg.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
15.0.dhcpmon.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.2.bGf2H3tXGg.exe.10000000.5.unpack	100%	Avira	HEUR/AGEN.1120893		Download File
14.0.bGf2H3tXGg.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
3.2.bGf2H3tXGg.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.2.dhcpmon.exe.4a60000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.1.bGf2H3tXGg.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.2.dhcpmon.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
backu4734.duckdns.org	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
backu4734.duckdns.org	1%	Virustotal		Browse
backu4734.duckdns.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
backu4734.duckdns.org	40.71.91.165	true	true	• 1%, Virustotal, Browse	unknown

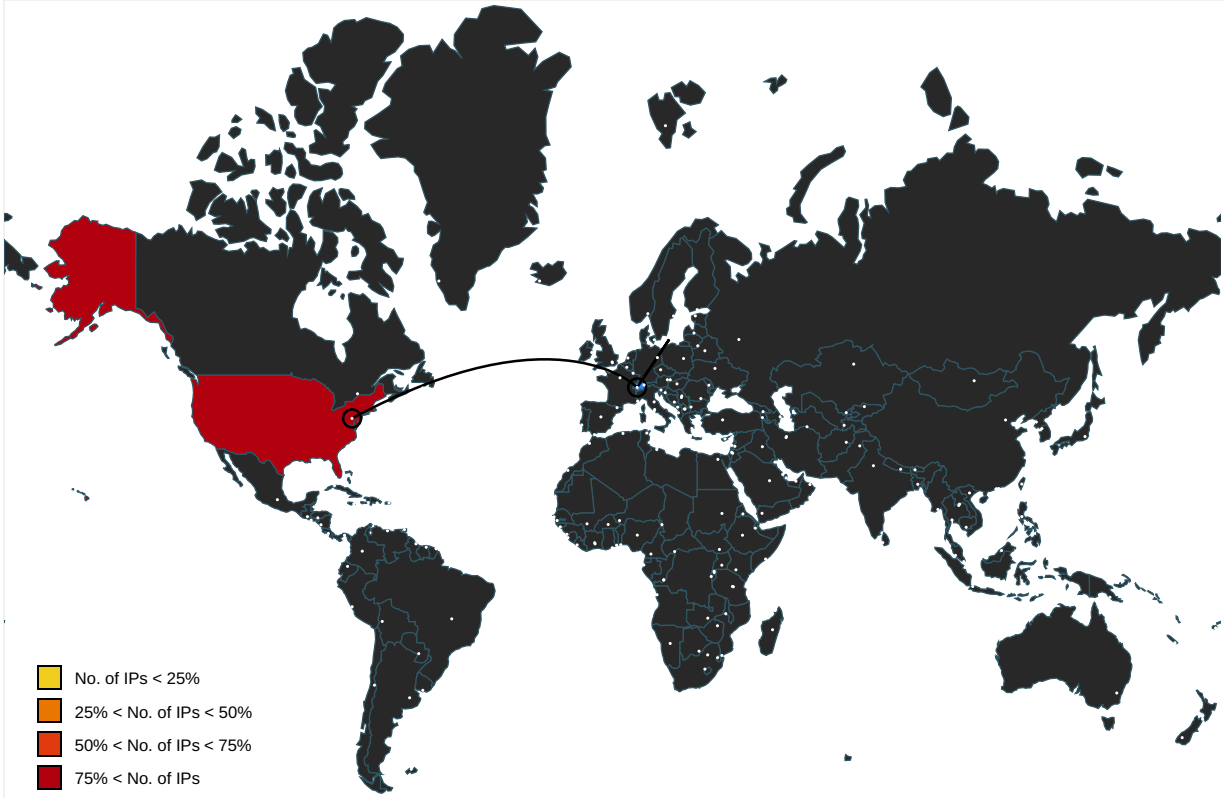
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
backu4734.duckdns.org	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_Error	bGf2H3tXGg.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	bGf2H3tXGg.exe	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
40.71.91.165	backu4734.duckdns.org	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384149
Start date:	08.04.2021
Start time:	17:20:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bGf2H3tXGg.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@18/24@16/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.5% (good quality ratio 12.3%) • Quality average: 75.8% • Quality standard deviation: 32.1%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 168.61.161.212, 104.42.151.234, 23.54.113.53, 104.43.193.48, 13.64.90.137, 95.100.54.203, 20.82.209.183, 23.10.249.43, 23.10.249.26, 20.82.210.154, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:21:09	API Interceptor	838x Sleep call for process: bGf2H3tXGg.exe modified
17:21:17	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\bGf2H3tXGg.exe" s>$(Arg0)
17:21:20	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
17:21:21	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
17:21:30	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
40.71.91.165	zr0evNqvkC.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
backu4734.duckdns.org	zr0evNqvkC.exe	Get hash	malicious	Browse	• 40.71.91.165

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MICROSOFT-CORP-MSN-AS-BLOCKUS	securedmessage.htm	Get hash	malicious	Browse	• 52.239.152.74
	Fattura di errore.exe	Get hash	malicious	Browse	• 104.209.133.4
	PaymentAdvice.exe	Get hash	malicious	Browse	• 52.142.208.184
	Signed pages of agreement copy.html	Get hash	malicious	Browse	• 52.97.232.194
	zr0evNqvkC.exe	Get hash	malicious	Browse	• 40.71.91.165
	uGSmoUM8Ex.exe	Get hash	malicious	Browse	• 52.169.150.217
	New Orders.exe	Get hash	malicious	Browse	• 104.209.133.4
	6r3kQ7Ddkk.dll	Get hash	malicious	Browse	• 204.79.197.200
	S9LQJCAiXi.exe	Get hash	malicious	Browse	• 40.122.131.23
	sample.exe	Get hash	malicious	Browse	• 40.91.125.204
	wzdu53.exe	Get hash	malicious	Browse	• 52.239.137.4
	bank details.exe	Get hash	malicious	Browse	• 20.43.32.222
	covid.exe	Get hash	malicious	Browse	• 168.62.194.64
	1drive.exe	Get hash	malicious	Browse	• 137.117.64.85
	onbgX3WswF.exe	Get hash	malicious	Browse	• 52.142.208.184
	scan-100218.docm	Get hash	malicious	Browse	• 51.145.124.145
	Honeywell Home_v5.3.0_apkpure.com_20201208.apk	Get hash	malicious	Browse	• 52.232.209.85
	bcex.apk.1	Get hash	malicious	Browse	• 52.175.56.158
	Transfer Form.exe	Get hash	malicious	Browse	• 20.43.32.222
	PaymentInvoice.exe	Get hash	malicious	Browse	• 52.142.208.184

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\bGf2H3tXGg.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	702907
Entropy (8bit):	5.903583773476114
Encrypted:	false
SSDEEP:	6144:69X0GFb/PdSrw+uHwUa5EIZUNf5F6p363E+r+voPIQLAoxQHHmAOZPBwf9:M0o1+Bvgs36pcoPIWPxUH1F
MD5:	F72A7FD231E50F9B43C3DAB470364846
SHA1:	1AC9F0876EC8F4B95FB0BBAE48C2A5B5D02ED411
SHA-256:	FB01157B437B00F34999FAA320BB55C8E44BDBB415E9A15503035BFE0E1D40D6
SHA-512:	C12BC1D2B74C2F209EADD40C02A56EE4B1A21287AB5B3391118F1FA12971C39DCBE2B8174B43A4D19281680247398140B223E0F00F03896B71AA8AA2352C084E
Malicious:	**true**

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 51%, Browse • Antivirus: Metadefender, Detection: 16%, Browse • Antivirus: ReversingLabs, Detection: 69%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG.sw..PG..VA..PG.Rich.PG .....PE..L...".$_.....f.....H3.....@.....0.....@.....D..... .....text...Wd.....f..... ..`.rdata.....j.....@..@.data...8U.....~.....@....ndata.....rsrc.....@..@..... ....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\bGf2H3tXGg.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\bGf2H3tXGg.exe.log	
Process:	C:\Users\user\Desktop\bGf2H3tXGg.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

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):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\nejus0or2e4wbg8rhay	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	data
Category:	dropped
Size (bytes):	283136
Entropy (8bit):	**7.999260184879652**
Encrypted:	**true**
SSDEEP:	6144:3w+uHwUa5EIZUNf5F6p363E+r+voPIQLAoxQHHmAOZPBwfY:g+Bvgs36pcoPIWPxUH1g
MD5:	285906EFB24E6C8780A7F2E30BDBE72A
SHA1:	5CBAE1392002A6956635E15DB5147F85620F30E8
SHA-256:	AF23271A22B4657CF3765BB7A1A40E130CB9145D4549D004CF9BAF1C4CB854CA
SHA-512:	BFC53D9B2047DB89CB5828C49C12CA68BB999F9633EE8FD11BB9E110634812F18137280E6DE79AFD1C3B83731E4F21F6300F92BFDD9917ED6576F3111144A8CI
Malicious:	false
Preview:	.\.5...x).....b?...k.1P&.....f.p...3..d.;.vR7.P...c....1...u.aH...hSE}...^&.@wL..DI.....l.`VS..v..J..*o.A...@..\..S#..aU ....%.....!l...Ym.V....#..r6..o..YbA.bN..../.....sj.T..EX..G...F...kG.}7#6x....<.}.....L..K.D..H.#a...~:_.'.....9M..\...).<..6.;.(..v.....d.P.4....H..c.m.s4-=..N.....l...,j'....Y.*.Ex..F.5c?..c>....qhq...#..>.nm.{.xp....$M.}.V.?[uY.(.&.TW..#..=...M.....k.....ln..W.j.cbX.....6F.D.>...x..K.:_.f3kD..l...^...q9.vW.@.3.OG..`.9...fPc..!..'c0.r.}.?...O...%.*.EY%H.+.y.]..D.f.:.....M.I...X=.1.U....K}.I...aY.N...c...M.....G.....8..dw.m...L..O.@^..a>.....?...[9.T"'..dO0..1.$.....?8..rs..n&U. h.[e...N. *h....T..MW$....!.&2...@.Y.bL..Gv.L...|.2....4{wEZ.iB....n.....P.6z.c...R.z...>.O#rr..p....H...O..NkjZ*w...'{..L....]]Q...s5...o....}.6.f.....)>R`.l.5A....{.A..z....'.b..A..];d.2.w..P...-.....X.>W#...0.o.#S2%..U..m..K.....h%...H.5A...Ul....:1....3.....A...iN...JI.C..=....Z..q.3.C..r..C..Y....}

C:\Users\user\AppData\Local\Temp\nsfEFEC.tmp\xktfu.dll	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.042717862409682
Encrypted:	false
SSDEEP:	48:a2f1CPWItdEEB+dlbcTeJjhaYLTxGCv402KcUlWG6QmtN1BbRuqS:InB+7cTkTxGCA02K74tp1x
MD5:	55ED3B347F615FAE9FB0D62EFA642861
SHA1:	2978295CFE6CB8ED8C7D7BCEBF0CB13DCD6C9256
SHA-256:	9C94096638FBAD8F4F41E33012437C149ECD4AB055E56FDDACBD35CBCB2ADCB6
SHA-512:	4AC65E360218AE12205C79C32C057B78065EFDD81C679B706694CE22A5F3838473897617E8C973DD738F312494B01082A4A292176CB6E00E5B29A110B0F2B3A5
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Virustotal, Detection: 19%, Browse • Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 41%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...>.f`.....!..... .....P.....A.....!..L...."....@..... ..... ..@..... .....text..... ..... ..`.rdata..... .....@..@.data...0....0.....@....rsrc.....@.....@..@.....

C:\Users\user\AppData\Local\Temp\nsh9AB8.tmp\xktfu.dll	
Process:	C:\Users\user\Desktop\bGf2H3tXGg.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.042717862409682
Encrypted:	false
SSDEEP:	48:a2f1CPWItdEEB+dlbcTeJjhaYLTxGCv402KcUlWG6QmtN1BbRuqS:InB+7cTkTxGCA02K74tp1x
MD5:	55ED3B347F615FAE9FB0D62EFA642861
SHA1:	2978295CFE6CB8ED8C7D7BCEBF0CB13DCD6C9256
SHA-256:	9C94096638FBAD8F4F41E33012437C149ECD4AB055E56FDDACBD35CBCB2ADCB6
SHA-512:	4AC65E360218AE12205C79C32C057B78065EFDD81C679B706694CE22A5F3838473897617E8C973DD738F312494B01082A4A292176CB6E00E5B29A110B0F2B3A5
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Virustotal, Detection: 19%, Browse • Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 41%

C:\Users\user\AppData\Local\Temp\nsh9AB8.tmp\xktfu.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L. ..>.f`.....!..... .....P.....A.....!..L...."....@..... ..@..... .....text..... ..... ..`.rdata..... .....@..@.data...0....0.....@....rsrc.....@.....@..@..... .....

C:\Users\user\AppData\Local\Temp\nsmE619.tmp\xktfu.dll	
Process:	C:\Users\user\Desktop\bGf2H3tXGg.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.042717862409682
Encrypted:	false
SSDEEP:	48:a2f1CPWItdEEB+dlbcTeJjhaYLTxGCv402KcUlWG6QmtN1BbRuqS:InB+7cTkTxGCA02K74tp1x
MD5:	55ED3B347F615FAE9FB0D62EFA642861
SHA1:	2978295CFE6CB8ED8C7D7BCEBF0CB13DCD6C9256
SHA-256:	9C94096638FBAD8F4F41E33012437C149ECD4AB055E56FDDACBD35CBCB2ADCB6
SHA-512:	4AC65E360218AE12205C79C32C057B78065EFDD81C679B706694CE22A5F3838473897617E8C973DD738F312494B01082A4A292176CB6E00E5B29A110B0F2B3A5
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Virustotal, Detection: 19%, Browse • Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 41%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L. ..>.f`.....!..... .....P.....A.....!..L...."....@..... ..@..... .....text..... ..... ..`.rdata..... .....@..@.data...0....0.....@....rsrc.....@.....@..@..... .....

C:\Users\user\AppData\Local\Temp\nsp1382.tmp\xktfu.dll	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.042717862409682
Encrypted:	false
SSDEEP:	48:a2f1CPWItdEEB+dlbcTeJjhaYLTxGCv402KcUlWG6QmtN1BbRuqS:InB+7cTkTxGCA02K74tp1x
MD5:	55ED3B347F615FAE9FB0D62EFA642861
SHA1:	2978295CFE6CB8ED8C7D7BCEBF0CB13DCD6C9256
SHA-256:	9C94096638FBAD8F4F41E33012437C149ECD4AB055E56FDDACBD35CBCB2ADCB6
SHA-512:	4AC65E360218AE12205C79C32C057B78065EFDD81C679B706694CE22A5F3838473897617E8C973DD738F312494B01082A4A292176CB6E00E5B29A110B0F2B3A5
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Virustotal, Detection: 19%, Browse • Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 41%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L. ..>.f`.....!..... .....P.....A.....!..L...."....@..... ..@..... .....text..... ..... ..`.rdata..... .....@..@.data...0....0.....@....rsrc.....@.....@..@..... .....

C:\Users\user\AppData\Local\Temp\tmpDE28.tmp	
Process:	C:\Users\user\Desktop\bGf2H3tXGg.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.109950989988902
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0POLxtn:cbk4oL600QydbQxIYODOLedq3SOj
MD5:	7F3B873F0BEBEC1CA523C1EA10D53D80
SHA1:	3EB161B07F5EF732D6C39DD6BC13E1C3AD3036E4
SHA-256:	E0932A6253B8851243AFF143973201F1F4D88A908DA580AFC1AB83A0EC043CDE
SHA-512:	8C8EB7B8FED0A52CBB0CFA4471C1A7780D50C8D249CD14F0FD590662046D6A6705968C66EDA96A4C0E58D0746E4B6BD9E485C4CDC06D630C7FEA2ECFB86AE 107
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\tmpDE28.tmp	
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\tmpE0E8.tmp	
Process:	C:\Users\user\Desktop\bGf2H3tXGg.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
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\Local\Temp\xavbedcnsrtbhix	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	data
Category:	dropped
Size (bytes):	11781
Entropy (8bit):	7.984459379386964
Encrypted:	false
SSDEEP:	192:pBenVpIMVi3Lb5zyZXE/yld/gQOEBaX0wZkWVAMrtFW0VzoiSrWP6WQpHWcJcNdD:yVCR52ZXs8dQ1RZkEAmtd1olYWHWcwIE
MD5:	BCB945B4C41466420E84B5CED1F7C5F4
SHA1:	5041C43DEBCC2B9E65D11D658F0FE8C8A45E074F
SHA-256:	B4BC8BCAFC597734DFF776D588DCF7F82C6BA6A1BA96F04A0B384B3F30AA4E24
SHA-512:	645EB26BA2E711C68A1982CB4D93A9432B610B64A92CAFA134ED7219272677F44B1BA7BC27F75FE94CBBB6EF5AA1EB8B33257391FB04FC1BDF04EA4997FFB621
Malicious:	false
Preview:	tD*@J..p.....>a..e.6q..{.r.w.z..E.LS.,_N....._..$....x.!#..l..P3-/."x&..X...4"T.....^....gqs...j",.C=?hf.v.8.OY[D..R../...P...`7.....r\|.....>H.....3.Z.o.....w.....O$. ..g...0:<M. '..m...-iM..=.....S.....K.e..#e..{3..{i.l../II.O..yO....K....k.E...y.W..".?....S...<.$.....<.....d...+%'.6p....7..,^L:..d...8HX...\|_ik...b.$.{uw`h.n&0.GQS|.J....HP.V.....jt.....~v@...5..HZ !...KP)*.3....9.....'.". ....4.0..6.. .68.u./BMkr.ef.....U...b3xEF`..vx35ENPZu.Xl....F....c.....I..l.....wl....KX.5..../j..(7..9...../J..}...)+..L1N/...../.n6(...^]7.....egq....OuLK]..{u2..n ..oa:.....G....^m.....szdj.t.#L....LN.....:.....1.....7.....,a2.....8.s8..u..C..q...`jl.[l.....oe^p'.>&..bE.F.j..V./...$.....r...y..{=....}....I[.....y.^AD.O.....K.....A/;5. -,9,.7..:.6.....p ..eugq>m.t{uw&.R3e.=AC..9S[U.SOO.....~....J...}t<.y.G.....lv...RP.....j[...,....D.....P....W..(....a..a.....aB<d.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\bGf2H3tXGg.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhDjhL
MD5:	30D23CC577A89146961915B57F408623
SHA1:	9B5709D6081D8E0A570511E6E0AAE96FA041964F
SHA-256:	E2130A72E55193D402B5F43F7F3584ECF6B423F8EC4B1B1B69AD693C7E0E5A9E
SHA-512:	2D5C5747FD04F8326C2CC1FB313925070BC01D3352AFA6C36C167B72757A15F58B6263D96BD606338DA055812E69DDB628A6E18D64DD59697C2F42D1C58CC68
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.....[.&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.....[.&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.....[.&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.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\bGf2H3tXGg.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:wFGet:wrt
MD5:	DF854956BB207377B050755321BC7605
SHA1:	1E82091BE0AD796EAF136C55B5AD83D650AE72CA
SHA-256:	0E92D96AF7FB340B34C5C7EEE2AEF7059B5B0181952CE900B27F8A8B8E0FEA2B
SHA-512:	BAB25B65AC0C3F2496924D04DBD89E32029C248350440BBB3C9EF6268AA7E389BFDD9F6982350B6CBD38B107B42D291801671B52129B47F075FC76EF1F128C2E
Malicious:	**true**
Preview:	.>.c...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\Desktop\bGf2H3tXGg.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F97
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\bGf2H3tXGg.exe
File Type:	data
Category:	modified
Size (bytes):	64
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYVsRLY6oRDT6P2bfVn1:RzWDIfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A6
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\bGf2H3tXGg.exe
File Type:	data
Category:	dropped
Size (bytes):	327768
Entropy (8bit):	**7.999367066417797**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3PlZmqze1d1wI8lkWmtjJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C3A
Malicious:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\bGf2H3tXGg.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	38
Entropy (8bit):	4.405822250285691
Encrypted:	false
SSDEEP:	3:oNUWJRWHSkV0Cn:oNNJApL
MD5:	0FB77C8DB46E53AD33B0288C4C8A4A14
SHA1:	3FE522409B1B18F07306B6F1691DD73D4B2A6212
SHA-256:	22C5A9F7013302D91E32B386E8B545BDDBB8F749FDC6CB403ACBB583FD3AD8C0
SHA-512:	98A7A9F58366F7C8BB237D0E73AF412105AF017240272B37D28F845C7C1BE26D7751769D0A83A2E485080C902903ABD48A7930D29A96964BB9820AA6754FED4D
Malicious:	false
Preview:	C:\Users\user\Desktop\bGf2H3tXGg.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	5.903583773476114
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:	bGf2H3tXGg.exe
File size:	702907
MD5:	f72a7fd231e50f9b43c3dab470364846
SHA1:	1ac9f0876ec8f4b95fb0bbae48c2a5b5d02ed411
SHA256:	fb01157b437b00f34999faa320bb55c8e44bdbb415e9a15503035bfe0e1d40d6
SHA512:	c12bc1d2b74c2f209eadd40c02a56ee4b1a21287ab5b3391118f1fa12971c39dcbe2b8174b43a4d19281680247398140b223e0f00f03896b71aa8aa2352c084e
SSDEEP:	6144:69X0GFb/PdSrw+uHwUa5EIZUNf5F6p363E+r+voPIQLAoxQHHmAOZPBwf9:M0o1+Bvgs36pcoPIWPxUH1F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L...".$_.....f.....H3.....@

File Icon

Icon Hash:	e0d8d8d4d4d8d0e8

Static PE Info

General

Entrypoint:	0x403348
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D722 [Sat Aug 1 02:44:50 2020 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:	ced282d9b261d1462772017fe2f6972b

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B8h]
call dword ptr [004080BCh]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042F42Ch], eax
je 00007F28E8708C83h
push ebx
call 00007F28E870BDE6h
cmp eax, ebx
je 00007F28E8708C79h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F28E870BD62h
push esi
call dword ptr [004080CCh]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F28E8708C5Dh
push 0000000Bh
call 00007F28E870BDBAh
push 00000009h
call 00007F28E870BDB3h
push 00000007h
mov dword ptr [0042F424h], eax
call 00007F28E870BDA7h
cmp eax, ebx
je 00007F28E8708C81h
push 0000001Eh
call eax
test eax, eax
je 00007F28E8708C79h
or byte ptr [0042F42Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx

Instruction
call dword ptr [00408288h]
mov dword ptr [0042F4F8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00429850h
call dword ptr [0040816Ch]
push 0040A188h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8544	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x5adc8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6457	0x6600	False	0.66823682598	data	6.43498570321	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1380	0x1400	False	0.4625	data	5.26100389731	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25538	0x600	False	0.463541666667	data	4.133728555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x5adc8	0x5ae00	False	0.0467997764787	data	2.65052430635	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x38280	0x42028	data		
RT_ICON	0x7a2a8	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x7a710	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x7ccb8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x7dd60	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x8e588	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_DIALOG	0x927b0	0x100	data	English	United States
RT_DIALOG	0x928b0	0x11c	data	English	United States
RT_DIALOG	0x929cc	0x60	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_GROUP_ICON	0x92a2c	0x5a	data		
RT_MANIFEST	0x92a88	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, ReadFile, GetTempFileNameA, WriteFile, RemoveDirectoryA, CreateProcessA, CreateFileA, GetLastError, CreateThread, CreateDirectoryA, GlobalUnlock, GetDiskFreeSpaceA, GlobalLock, SetErrorMode, GetVersion, lstrcpynA, GetCommandLineA, GetTempPathA, lstrlenA, SetEnvironmentVariableA, ExitProcess, GetWindowsDirectoryA, GetCurrentProcess, GetModuleFileNameA, CopyFileA, GetTickCount, Sleep, GetFileSize, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 70

- 53 (DNS)
- 8092 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 17:21:19.430593967 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:19.532866955 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:19.533004999 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:19.573600054 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:19.693836927 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:19.693979979 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:19.836230993 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:19.836409092 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:19.940630913 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:19.953306913 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.106357098 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.116871119 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.116904974 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.116926908 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.116954088 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.117017984 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.117078066 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.219286919 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.219361067 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.219405890 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.219470978 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.219481945 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.219507933 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.219527960 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.219541073 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.219568968 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.219598055 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.219620943 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.219640970 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.324055910 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.324091911 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.324115038 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.324136019 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.324157000 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.324179888 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.324191093 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.324202061 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.324229002 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.324234962 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.324245930 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.324254990 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.324276924 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.324300051 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.324325085 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.324326038 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.324341059 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.324347973 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.324368000 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.324373007 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.324394941 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.324421883 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.324435949 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.324457884 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.426434994 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.426480055 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.426508904 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.426534891 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.426575899 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.426613092 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.426630020 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.426719904 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.426748991 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.426774025 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.426779985 CEST	49708	8092	192.168.2.5	40.71.91.165

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 17:21:20.426826000 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.426866055 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.426896095 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.426933050 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.426947117 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.426964998 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427022934 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427048922 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427067995 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.427078009 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427104950 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427105904 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.427133083 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427146912 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.427161932 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427195072 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427242994 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.427277088 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427586079 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427612066 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427658081 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.427669048 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427670956 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.427755117 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427784920 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427817106 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427830935 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.427848101 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427860022 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.427876949 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427902937 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427927017 CEST	49708	8092	192.168.2.5	40.71.91.165
Apr 8, 2021 17:21:20.427942991 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427963018 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427989006 CEST	8092	49708	40.71.91.165	192.168.2.5
Apr 8, 2021 17:21:20.427989006 CEST	49708	8092	192.168.2.5	40.71.91.165

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 17:20:52.777942896 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:20:52.792874098 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 8, 2021 17:20:52.908107042 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:20:52.920916080 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 8, 2021 17:20:53.738787889 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:20:53.753365040 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 8, 2021 17:20:54.499186993 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:20:54.512229919 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 8, 2021 17:20:54.952914000 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:20:54.971004009 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 8, 2021 17:21:03.811711073 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:21:03.824161053 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 8, 2021 17:21:04.628942966 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:21:04.642151117 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 8, 2021 17:21:06.808931112 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:21:06.822011948 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 8, 2021 17:21:07.621742010 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:21:07.634968996 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 8, 2021 17:21:09.236407995 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:21:09.249181986 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 8, 2021 17:21:16.772994041 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:21:16.785816908 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 8, 2021 17:21:17.609308958 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:21:17.623075962 CEST	53	65296	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 17:21:19.230293989 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:21:19.411761999 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 8, 2021 17:21:20.604794979 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:21:20.645472050 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 8, 2021 17:21:29.107058048 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:21:29.293220043 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 8, 2021 17:21:34.792303085 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:21:34.808309078 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 8, 2021 17:21:41.324934959 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:21:41.338340998 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 8, 2021 17:21:44.674228907 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:21:44.686163902 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 8, 2021 17:21:48.354012966 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:21:48.535795927 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 8, 2021 17:21:55.362834930 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:21:55.377132893 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 8, 2021 17:21:57.871968031 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:21:57.891774893 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 8, 2021 17:22:01.625776052 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:22:01.638365984 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 8, 2021 17:22:07.701024055 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:22:07.714009047 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 8, 2021 17:22:14.676337957 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:22:14.888746977 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 8, 2021 17:22:19.713126898 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:22:19.727790117 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 8, 2021 17:22:25.775541067 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:22:25.788817883 CEST	53	58530	8.8.8.8	192.168.2.5
Apr 8, 2021 17:22:31.701319933 CEST	53813	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:22:31.715224028 CEST	53	53813	8.8.8.8	192.168.2.5
Apr 8, 2021 17:22:33.610249043 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:22:33.791585922 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 8, 2021 17:22:34.250060081 CEST	57344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:22:34.270764112 CEST	53	57344	8.8.8.8	192.168.2.5
Apr 8, 2021 17:22:39.213460922 CEST	54450	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:22:39.231551886 CEST	53	54450	8.8.8.8	192.168.2.5
Apr 8, 2021 17:22:40.763470888 CEST	59261	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:22:40.776850939 CEST	53	59261	8.8.8.8	192.168.2.5
Apr 8, 2021 17:22:47.613575935 CEST	57151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:22:47.627650023 CEST	53	57151	8.8.8.8	192.168.2.5
Apr 8, 2021 17:22:51.380856037 CEST	59413	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:22:51.408750057 CEST	53	59413	8.8.8.8	192.168.2.5
Apr 8, 2021 17:22:53.967757940 CEST	60516	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:22:53.981085062 CEST	53	60516	8.8.8.8	192.168.2.5
Apr 8, 2021 17:23:00.772382021 CEST	51649	53	192.168.2.5	8.8.8.8
Apr 8, 2021 17:23:00.785746098 CEST	53	51649	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 17:21:19.230293989 CEST	192.168.2.5	8.8.8.8	0x42a	Standard query (0)	backu4734.duckdns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 17:21:29.107058048 CEST	192.168.2.5	8.8.8.8	0x22b0	Standard query (0)	backu4734.duckdns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 17:21:34.792303085 CEST	192.168.2.5	8.8.8.8	0x6924	Standard query (0)	backu4734.duckdns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 17:21:41.324934959 CEST	192.168.2.5	8.8.8.8	0xc909	Standard query (0)	backu4734.duckdns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 17:21:48.354012966 CEST	192.168.2.5	8.8.8.8	0x1522	Standard query (0)	backu4734.duckdns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 17:21:55.362834930 CEST	192.168.2.5	8.8.8.8	0xbe28	Standard query (0)	backu4734.duckdns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:01.625776052 CEST	192.168.2.5	8.8.8.8	0xb9fe	Standard query (0)	backu4734.duckdns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:07.701024055 CEST	192.168.2.5	8.8.8.8	0x8a6	Standard query (0)	backu4734.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 17:22:14.676337957 CEST	192.168.2.5	8.8.8.8	0xd02a	Standard query (0)	backu4734.duckdns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:19.713126898 CEST	192.168.2.5	8.8.8.8	0xab6a	Standard query (0)	backu4734.duckdns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:25.775541067 CEST	192.168.2.5	8.8.8.8	0xafbf	Standard query (0)	backu4734.duckdns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:33.610249043 CEST	192.168.2.5	8.8.8.8	0x47e1	Standard query (0)	backu4734.duckdns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:40.763470888 CEST	192.168.2.5	8.8.8.8	0x9db0	Standard query (0)	backu4734.duckdns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:47.613575935 CEST	192.168.2.5	8.8.8.8	0x6edc	Standard query (0)	backu4734.duckdns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:53.967757940 CEST	192.168.2.5	8.8.8.8	0x116f	Standard query (0)	backu4734.duckdns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 17:23:00.772382021 CEST	192.168.2.5	8.8.8.8	0x73b1	Standard query (0)	backu4734.duckdns.org	A (IP address)	IN (0x0001)

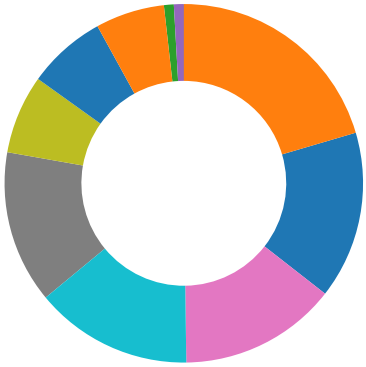
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 17:21:19.411761999 CEST	8.8.8.8	192.168.2.5	0x42a	No error (0)	backu4734.duckdns.org		40.71.91.165	A (IP address)	IN (0x0001)
Apr 8, 2021 17:21:29.293220043 CEST	8.8.8.8	192.168.2.5	0x22b0	No error (0)	backu4734.duckdns.org		40.71.91.165	A (IP address)	IN (0x0001)
Apr 8, 2021 17:21:34.808309078 CEST	8.8.8.8	192.168.2.5	0x6924	No error (0)	backu4734.duckdns.org		40.71.91.165	A (IP address)	IN (0x0001)
Apr 8, 2021 17:21:41.338340998 CEST	8.8.8.8	192.168.2.5	0xc909	No error (0)	backu4734.duckdns.org		40.71.91.165	A (IP address)	IN (0x0001)
Apr 8, 2021 17:21:48.535795927 CEST	8.8.8.8	192.168.2.5	0x1522	No error (0)	backu4734.duckdns.org		40.71.91.165	A (IP address)	IN (0x0001)
Apr 8, 2021 17:21:55.377132893 CEST	8.8.8.8	192.168.2.5	0xbe28	No error (0)	backu4734.duckdns.org		40.71.91.165	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:01.638365984 CEST	8.8.8.8	192.168.2.5	0xb9fe	No error (0)	backu4734.duckdns.org		40.71.91.165	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:07.714009047 CEST	8.8.8.8	192.168.2.5	0x8a6	No error (0)	backu4734.duckdns.org		40.71.91.165	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:14.888746977 CEST	8.8.8.8	192.168.2.5	0xd02a	No error (0)	backu4734.duckdns.org		40.71.91.165	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:19.727790117 CEST	8.8.8.8	192.168.2.5	0xab6a	No error (0)	backu4734.duckdns.org		40.71.91.165	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:25.788817883 CEST	8.8.8.8	192.168.2.5	0xafbf	No error (0)	backu4734.duckdns.org		40.71.91.165	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:33.791585922 CEST	8.8.8.8	192.168.2.5	0x47e1	No error (0)	backu4734.duckdns.org		40.71.91.165	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:40.776850939 CEST	8.8.8.8	192.168.2.5	0x9db0	No error (0)	backu4734.duckdns.org		40.71.91.165	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:47.627650023 CEST	8.8.8.8	192.168.2.5	0x6edc	No error (0)	backu4734.duckdns.org		40.71.91.165	A (IP address)	IN (0x0001)
Apr 8, 2021 17:22:53.981085062 CEST	8.8.8.8	192.168.2.5	0x116f	No error (0)	backu4734.duckdns.org		40.71.91.165	A (IP address)	IN (0x0001)
Apr 8, 2021 17:23:00.785746098 CEST	8.8.8.8	192.168.2.5	0x73b1	No error (0)	backu4734.duckdns.org		40.71.91.165	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: bGf2H3tXGg.exe PID: 4656 Parent PID: 5736

General

Start time:	17:20:58
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\bGf2H3tXGg.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\bGf2H3tXGg.exe'
Imagebase:	0x400000
File size:	702907 bytes
MD5 hash:	F72A7FD231E50F9B43C3DAB470364846
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: 00000000.00000002.255989903.00000000029B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.255989903.00000000029B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.255989903.00000000029B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.255989903.00000000029B0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsr9A59.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\xavbedcnsrtbhix	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Local\Temp\nejus0or2e4wbg8rhay	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Local\Temp\nsh9AB8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsh9AB8.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40572D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsh9AB8.tmp\xktfu.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsr9A59.tmp	success or wait	1	4035BF	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsh9AB8.tmp	success or wait	1	4058EE	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xavbedcnsrtbhix	unknown	11781	74 44 2a 40 4a de 03 70 b3 09 87 00 0b 8d 9e 9d ab 0c 9e b7 3e 61 e0 b0 e5 b4 ae 65 f4 84 36 71 fc 8c 7b c2 72 fc 77 ca 7a 8a 86 45 d4 4c 53 9a 2c 5f 4e df 04 a1 8e f2 9a a4 9e ef f9 c2 f0 5f c1 f0 24 10 be b5 7f 78 d7 21 23 cc 18 6c da 91 9b 50 33 2d 2f d8 22 78 26 de e8 58 ff 09 0b 34 22 54 02 fa c4 b0 1b 15 17 00 5e a0 0e c6 d0 b8 67 71 73 1c 0c bc 6a 22 2c 90 43 3d 3f 68 66 88 76 2e 38 d7 4f 59 5b 44 ac e3 52 0a 14 2f ab a5 a7 50 b0 ef 9e 16 60 37 b7 81 83 ac b2 cb ba 72 7c 0f 93 8d 8f b8 ae d7 86 3e 48 17 e0 ea ec 94 05 33 e1 5a a4 6f fc f6 f8 df e7 ff ed a6 b0 77 c8 d2 d4 fb d9 1b c9 82 8c 4f 24 1e 20 c7 cf 67 d5 8e 98 17 30 3a 3c 4d b2 27 df f1 6d 0a 0c 06 2d 69 4d 03 fb 3d f5 03 01 a3 11 c9 53 c7 11 ff b1 17 cf a1 d1 17 4b b7 65 1d a7 23 65 b5 85	tD*@J..p.....>a.....e.. 6q..{.r.w.z..E.LS.,_N..... ..._..$....x.!#..I...P3-/."x&. .X...4"T.....^.....gqs...j" ,.C=? hf.v.8.OY[D..R../...P.... `7.....r\|.....>H.....3.Z .o.....w.....O$. ..g....0: <M.'..m...-iM..=.....S... .....K.e..#e..	success or wait	1	405D51	WriteFile
C:\Users\user\AppData\Local\Temp\nejus0or2e4wbg8rhay	unknown	32768	fa 5c 85 35 c1 06 e8 b7 78 29 06 b7 12 e5 10 62 3f ad bd ba 6b ad 31 50 26 e0 aa 0f 12 c5 da a7 82 a0 e6 66 9a 70 91 10 83 33 ba fd 64 b8 3b 9f 76 52 37 db 50 bd fb 99 63 0a a1 9a a8 31 d8 8a b9 b2 75 19 61 48 dc 19 80 68 53 45 7d aa ac 08 5e 26 ce 40 77 4c e3 c1 44 49 bb 8b 97 de bd 04 c9 04 16 ab 49 ef a2 60 56 53 e7 ef 76 b3 ef 4a 86 92 2a 6f 7f 41 d7 ea 0d 40 ff 97 5c 0f f8 53 23 91 1e 61 55 20 af 87 a2 a4 25 9a 97 1a b4 de f0 21 49 9a a6 83 59 6d dd 56 bf a6 a8 d2 b7 23 d3 c7 72 36 d8 1b 6f da 0b 59 62 41 99 62 4e 0a e9 0a e2 2f 00 0f 1c bc b6 73 6a 8e 54 81 8c 45 58 1d 2e 47 05 8d 1d 46 1b fa f9 6b 47 92 7d 37 23 36 78 81 1f b6 83 3c 05 7d 16 93 01 f8 ae f0 4c d8 18 4b ac 44 85 e7 a5 b3 48 fb 23 61 05 b0 d8 7e 3a 5f fb 27 8e ea dd e5 87 e6 15 c8 df	.\.5....x).....b?...k.1P&..... .....f.p...3..d.;.vR7.P...c... .1....u.aH...hSE}...^&.@wL. .DI.....I..`VS..v..J..*o.A.. .@..\..S#..aU ....%.....!I... Ym.V.....#..r6..o..YbA.bN... ./ .....sj.T..EX..G...F...kG.}7# 6x....<.}.....L..K.D....H.#a.. .~:_.'.....	success or wait	9	405D51	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsh9AB8.tmp\xktfu.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 3e 92 66 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0e 10 00 04 00	MZ......................@....... ....!..L.!This program cannot be run in DOS mode.... $............................ ....PE..L...>.f`.... ....!.......	success or wait	1	405D51	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\bGf2H3tXGg.exe	unknown	512	success or wait	794	405D22	ReadFile
C:\Users\user\Desktop\bGf2H3tXGg.exe	unknown	4	success or wait	2	405D22	ReadFile
C:\Users\user\Desktop\bGf2H3tXGg.exe	unknown	4	success or wait	14	405D22	ReadFile
C:\Users\user\AppData\Local\Temp\xavbedcnsrtbhix	unknown	11781	success or wait	1	10001221	ReadFile
C:\Users\user\AppData\Local\Temp\nejus0or2e4wbg8rhay	unknown	283136	success or wait	1	22820B5	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	228085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	228085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	228085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	228085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	228085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	228085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	228085D	ReadFile

Analysis Process: bGf2H3tXGg.exe PID: 204 Parent PID: 4656

General

Start time:	17:21:09
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\bGf2H3tXGg.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\bGf2H3tXGg.exe'
Imagebase:	0x400000
File size:	702907 bytes
MD5 hash:	F72A7FD231E50F9B43C3DAB470364846
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: 00000003.00000002.494409950.0000000004E72000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.494409950.0000000004E72000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.494409950.0000000004E72000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000001.247277523.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000001.247277523.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000001.247277523.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.488378947.00000000021D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.488378947.00000000021D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.488378947.00000000021D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.488378947.00000000021D0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.493792875.00000000036D7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.488999685.00000000023D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.489075151.000000000243C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.485375087.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.485375087.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.485375087.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.485375087.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.486901430.0000000000658000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.486901430.0000000000658000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.486901430.0000000000658000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.493192985.0000000003464000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCFCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCFCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C9BBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C9B1E60	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C9BBEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C9BDD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C9BDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpDE28.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C9B7038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C9B1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpE0E8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C9B7038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C9BBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C9BBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	14	6C9B1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C9B1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C9B1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6C9BDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpDE28.tmp	success or wait	1	6C9B6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE0E8.tmp	success or wait	1	6C9B6A95	DeleteFileW
C:\Users\user\Desktop\bGf2H3tXGg.exe:Zone.Identifier	success or wait	1	5148BA6	DeleteFileA
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	success or wait	1	6C9B6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	df 3e e0 63 ed fa d8 48	.>.c...H	success or wait	1	6C9B1B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 ad 31 29 81 e9 50 47 d2 e9 50 47 d2 e9 50 47 d2 2a 5f 18 d2 eb 50 47 d2 e9 50 46 d2 49 50 47 d2 2a 5f 1a d2 e6 50 47 d2 bd 73 77 d2 e3 50 47 d2 2e 56 41 d2 e8 50 47 d2 52 69 63 68 e9 50 47 d2 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 22 d7 24 5f 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 66 00 00 00 1e 08 00 00 04 00 00 48 33 00 00 00 10 00 00 00 80 00 00 00 00 40	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........1)..PG..PG..PG.*_... P G..PF.IPG.*_...PG..sw..PG ..VA. .PG.Rich.PG.........PE..L..." .$_.................f.......... H3............@	success or wait	3	6C9BDD66	CopyFileW
C:\Program Files (x86)\DHCP Mo nitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C9BDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpDE28.tmp	unknown	1301	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveTo ken</LogonType>	success or wait	1	6C9B1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	38	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 44 65 73 6b 74 6f 70 5c 62 47 66 32 48 33 74 58 47 67 2e 65 78 65	C:\Users\user\Desktop\bGf2H3tXGg.exe	success or wait	1	6C9B1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpE0E8.tmp	unknown	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?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>	success or wait	1	6C9B1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 7e 66 1e 47 30 5e c3 a9 dd 96 3b b4 2e 95 a2 57 32 c2 3d 10 b3 ce 4b ca 7e c7 4c cc 9f 15 26 66 8d bb 2e 70 c8 04 1b f8 b7 c2 0f e9 ff e7 0b 10 3a 37 72 48 7d bd be f1 88 0d 2f 48 16 b2 87 06 17 96 4c 8c b6 04 3f b5 f3 04 41 08 4b 07 d1 e5 84 4a 17 3d 38 78 21 19 a1 e1 e4 2b fa 32 65 27 d7 1f 45 3f d9 47 11 9e a7 e7 a8 01 f0 5b 00 26	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.....[.&	success or wait	8	6C9B1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327768	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wpK .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_...Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...l.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6C9B1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	24	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d f0 4a 22 83 43 3b 22 61	9iH....}Z..4..f..J".C;"a	success or wait	1	6C9B1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	0	24	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d f0 4a 22 83 43 3b 22 61	9iH....}Z..4..f..J".C;"a	success or wait	1	6C9BDD66	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6C9B1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C9B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C9B1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DCBD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DCBD72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6C9B646A	RegSetValueExW

Analysis Process: schtasks.exe PID: 6280 Parent PID: 204

General

Start time:	17:21:16
Start date:	08/04/2021
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\tmpDE28.tmp'
Imagebase:	0xb50000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpDE28.tmp	unknown	2	success or wait	1	B5AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpDE28.tmp	unknown	1302	success or wait	1	B5ABD9	ReadFile

Analysis Process: conhost.exe PID: 6288 Parent PID: 6280

General

Start time:	17:21:16
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 6320 Parent PID: 204

General

Start time:	17:21:17
Start date:	08/04/2021
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\tmpE0E8.tmp'
Imagebase:	0x7ff797770000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE0E8.tmp	unknown	2	success or wait	1	B5AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE0E8.tmp	unknown	1311	success or wait	1	B5ABD9	ReadFile

Analysis Process: conhost.exe PID: 6456 Parent PID: 6320

General

Start time:	17:21:17
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: bGf2H3tXGg.exe PID: 6468 Parent PID: 904

General

Start time:	17:21:17
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\bGf2H3tXGg.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\bGf2H3tXGg.exe 0
Imagebase:	0x400000
File size:	702907 bytes
MD5 hash:	F72A7FD231E50F9B43C3DAB470364846
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: 0000000B.00000002.306005261.00000000029B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.306005261.00000000029B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.306005261.00000000029B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.306005261.00000000029B0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nswE5BA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsmE619.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsmE619.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40572D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsmE619.tmp\xktfu.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nswE5BA.tmp	success or wait	1	4035BF	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsmE619.tmp	success or wait	1	4058EE	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xavbedcnsrtbhix	unknown	11781	74 44 2a 40 4a de 03 70 b3 09 87 00 0b 8d 9e 9d ab 0c 9e b7 3e 61 e0 b0 e5 b4 ae 65 f4 84 36 71 fc 8c 7b c2 72 fc 77 ca 7a 8a 86 45 d4 4c 53 9a 2c 5f 4e df 04 a1 8e f2 9a a4 9e ef f9 c2 f0 5f c1 f0 24 10 be b5 7f 78 d7 21 23 cc 18 6c da 91 9b 50 33 2d 2f d8 22 78 26 de e8 58 ff 09 0b 34 22 54 02 fa c4 b0 1b 15 17 00 5e a0 0e c6 d0 b8 67 71 73 1c 0c bc 6a 22 2c 90 43 3d 3f 68 66 88 76 2e 38 d7 4f 59 5b 44 ac e3 52 0a 14 2f ab a5 a7 50 b0 ef 9e 16 60 37 b7 81 83 ac b2 cb ba 72 7c 0f 93 8d 8f b8 ae d7 86 3e 48 17 e0 ea ec 94 05 33 e1 5a a4 6f fc f6 f8 df e7 ff ed a6 b0 77 c8 d2 d4 fb d9 1b c9 82 8c 4f 24 1e 20 c7 cf 67 d5 8e 98 17 30 3a 3c 4d b2 27 df f1 6d 0a 0c 06 2d 69 4d 03 fb 3d f5 03 01 a3 11 c9 53 c7 11 ff b1 17 cf a1 d1 17 4b b7 65 1d a7 23 65 b5 85	tD*@J..p.....>a.....e.. 6q..{.r.w.z..E.LS.,_N..... ..._..$....x.!#..l...P3-/."x&. .X...4"T.....^.....gqs...j" ,.C=? hf.v.8.OY[D..R../...P.... `7.....r\|.....>H.....3.Z .o.....w.....O$. ..g....0: <M.'..m...-iM..=.....S... .....K.e..#e..	success or wait	1	405D51	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nejus0or2e4wbg8rhay	unknown	32768	fa 5c 85 35 c1 06 e8 b7 78 29 06 b7 12 e5 10 62 3f ad bd ba 6b ad 31 50 26 e0 aa 0f 12 c5 da a7 82 a0 e6 66 9a 70 91 10 83 33 ba fd 64 b8 3b 9f 76 52 37 db 50 bd fb 99 63 0a a1 9a a8 31 d8 8a b9 b2 75 19 61 48 dc 19 80 68 53 45 7d aa ac 08 5e 26 ce 40 77 4c e3 c1 44 49 bb 8b 97 de bd 04 c9 04 16 ab 49 ef a2 60 56 53 e7 ef 76 b3 ef 4a 86 92 2a 6f 7f 41 d7 ea 0d 40 ff 97 5c 0f f8 53 23 91 1e 61 55 20 af 87 a2 a4 25 9a 97 1a b4 de f0 21 49 9a a6 83 59 6d dd 56 bf a6 a8 d2 b7 23 d3 c7 72 36 d8 1b 6f da 0b 59 62 41 99 62 4e 0a e9 0a e2 2f 00 0f 1c bc b6 73 6a 8e 54 81 8c 45 58 1d 2e 47 05 8d 1d 46 1b fa f9 6b 47 92 7d 37 23 36 78 81 1f b6 83 3c 05 7d 16 93 01 f8 ae f0 4c d8 18 4b ac 44 85 e7 a5 b3 48 fb 23 61 05 b0 d8 7e 3a 5f fb 27 8e ea dd e5 87 e6 15 c8 df	.\.5....x).....b?...k.1P&..... .....f.p...3..d.;.vR7.P...c... .1....u.aH...hSE}...^&.@wL. .DI..........I..`VS..v..J..*o.A.. .@..\..S#..aU ....%......!I... Ym.V.....#..r6..o..YbA.bN... ./ .....sj.T..EX..G...F...kG.}7# 6x....<.}......L..K.D....H.#a.. .~:_.'.........	success or wait	9	405D51	WriteFile
C:\Users\user\AppData\Local\Temp\nsmE619.tmp\xktfu.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 3e 92 66 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0e 10 00 04 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............................ ....PE..L...>.f`.... ....!.......	success or wait	1	405D51	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\bGf2H3tXGg.exe	unknown	512	success or wait	794	405D22	ReadFile
C:\Users\user\Desktop\bGf2H3tXGg.exe	unknown	4	success or wait	2	405D22	ReadFile
C:\Users\user\Desktop\bGf2H3tXGg.exe	unknown	4	success or wait	14	405D22	ReadFile
C:\Users\user\AppData\Local\Temp\xavbedcnsrtbhix	unknown	11781	success or wait	1	10001221	ReadFile
C:\Users\user\AppData\Local\Temp\nejus0or2e4wbg8rhay	unknown	283136	success or wait	1	29920B5	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	299085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	299085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	299085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	299085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	299085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	299085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	299085D	ReadFile

Analysis Process: dhcpmon.exe PID: 6600 Parent PID: 904

General

Start time:	17:21:20
Start date:	08/04/2021
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:	702907 bytes
MD5 hash:	F72A7FD231E50F9B43C3DAB470364846
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.00000002.311997780.00000000028B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.311997780.00000000028B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.311997780.00000000028B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.311997780.00000000028B0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 51%, Virustotal, Browse • Detection: 16%, Metadefender, Browse • Detection: 69%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsaEF7E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsfEFEC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsfEFEC.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40572D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsfEFEC.tmp\xktfu.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsaEF7E.tmp	success or wait	1	4035BF	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsfEFEC.tmp	success or wait	1	4058EE	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xavbedcnsrtbhix	unknown	11781	74 44 2a 40 4a de 03 70 b3 09 87 00 0b 8d 9e 9d ab 0c 9e b7 3e 61 e0 b0 e5 b4 ae 65 f4 84 36 71 fc 8c 7b c2 72 fc 77 ca 7a 8a 86 45 d4 4c 53 9a 2c 5f 4e df 04 a1 8e f2 9a a4 9e ef f9 c2 f0 5f c1 f0 24 10 be b5 7f 78 d7 21 23 cc 18 6c da 91 9b 50 33 2d 2f d8 22 78 26 de e8 58 ff 09 0b 34 22 54 02 fa c4 b0 1b 15 17 00 5e a0 0e c6 d0 b8 67 71 73 1c 0c bc 6a 22 2c 90 43 3d 3f 68 66 88 76 2e 38 d7 4f 59 5b 44 ac e3 52 0a 14 2f ab a5 a7 50 b0 ef 9e 16 60 37 b7 81 83 ac b2 cb ba 72 7c 0f 93 8d 8f b8 ae d7 86 3e 48 17 e0 ea ec 94 05 33 e1 5a a4 6f fc f6 f8 df e7 ff ed a6 b0 77 c8 d2 d4 fb d9 1b c9 82 8c 4f 24 1e 20 c7 cf 67 d5 8e 98 17 30 3a 3c 4d b2 27 df f1 6d 0a 0c 06 2d 69 4d 03 fb 3d f5 03 01 a3 11 c9 53 c7 11 ff b1 17 cf a1 d1 17 4b b7 65 1d a7 23 65 b5 85	tD*@J..p.....>a.....e.. 6q..{.r.w.z..E.LS.,_N..... ..._..$....x.!#..l...P3-/."x&. .X...4"T.....^.....gqs...j" ,.C=? hf.v.8.OY[D..R../...P.... `7.....r|.....>H.....3.Z .o.....w.....O$. ..g....0: <M.'..m...-iM..=.....S... .....K.e..#e..	success or wait	1	405D51	WriteFile
C:\Users\user\AppData\Local\Temp\nejus0or2e4wbg8rhay	unknown	32768	fa 5c 85 35 c1 06 e8 b7 78 29 06 b7 12 e5 10 62 3f ad bd ba 6b ad 31 50 26 e0 aa 0f 12 c5 da a7 82 a0 e6 66 9a 70 91 10 83 33 ba fd 64 b8 3b 9f 76 52 37 db 50 bd fb 99 63 0a a1 9a a8 31 d8 8a b9 b2 75 19 61 48 dc 19 80 68 53 45 7d aa ac 08 5e 26 ce 40 77 4c e3 c1 44 49 bb 8b 97 de bd 04 c9 04 16 ab 49 ef a2 60 56 53 e7 ef 76 b3 ef 4a 86 92 2a 6f 7f 41 d7 ea 0d 40 ff 97 5c 0f f8 53 23 91 1e 61 55 20 af 87 a2 a4 25 9a 97 1a b4 de f0 21 49 9a a6 83 59 6d dd 56 bf a6 a8 d2 b7 23 d3 c7 72 36 d8 1b 6f da 0b 59 62 41 99 62 4e 0a e9 0a e2 2f 00 0f 1c bc b6 73 6a 8e 54 81 8c 45 58 1d 2e 47 05 8d 1d 46 1b fa f9 6b 47 92 7d 37 23 36 78 81 1f b6 83 3c 05 7d 16 93 01 f8 ae f0 4c d8 18 4b ac 44 85 e7 a5 b3 48 fb 23 61 05 b0 d8 7e 3a 5f fb 27 8e ea dd e5 87 e6 15 c8 df	.\.5....x).....b?...k.1P&..... .....f.p...3..d.;.vR7.P...c... .1....u.aH...hSE}...^&.@wL. .DI.....I..`VS..v..J..*o.A.. .@..\..S#..aU ....%.....!I... Ym.V.....#..r6..o..YbA.bN... ./ .....sj.T..EX..G...F...kG.}7# 6x....<.}.....L..K.D....H.#a.. .~:_.'.....	success or wait	9	405D51	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsfEFEC.tmp\xktfu.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 3e 92 66 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0e 10 00 04 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............................ ....PE..L...>.f`.... ....!.......	success or wait	1	405D51	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	512	success or wait	782	405D22	ReadFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	4	success or wait	14	405D22	ReadFile
C:\Users\user\AppData\Local\Temp\xavbedcnsrtbhix	unknown	11781	success or wait	1	10001221	ReadFile
C:\Users\user\AppData\Local\Temp\nejus0or2e4wbg8rhay	unknown	283136	success or wait	1	24420B5	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	244085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	244085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	244085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	244085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	244085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	244085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	244085D	ReadFile

Analysis Process: bGf2H3tXGg.exe PID: 6704 Parent PID: 6468

General

Start time:	17:21:28
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\bGf2H3tXGg.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\bGf2H3tXGg.exe 0
Imagebase:	0x400000
File size:	702907 bytes
MD5 hash:	F72A7FD231E50F9B43C3DAB470364846
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.00000002.318797223.00000000034E1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.318797223.00000000034E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.318797223.00000000034E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.318707635.00000000024E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.317545365.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.317545365.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.317545365.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.317545365.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000001.300644075.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000001.300644075.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000001.300644075.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.319988300.0000000004A82000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.319988300.0000000004A82000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.319988300.0000000004A82000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.318495205.0000000000859000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.318495205.0000000000859000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.318495205.0000000000859000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.318765961.0000000002530000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.319780906.0000000004960000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.319780906.0000000004960000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.319780906.0000000004960000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.319780906.0000000004960000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.318855204.000000000351C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.318855204.000000000351C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCFCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCFCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\bGf2H3tXGg.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E00C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\bGf2H3tXGg.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E00C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C9B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C9B1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: 6752 Parent PID: 3472

General

Start time:	17:21:29
Start date:	08/04/2021
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:	702907 bytes
MD5 hash:	F72A7FD231E50F9B43C3DAB470364846
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: 0000000F.00000002.324052877.0000000002870000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.324052877.0000000002870000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.324052877.0000000002870000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.324052877.0000000002870000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nse1342.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsp1382.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsp1382.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40572D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsp1382.tmp\xktfu.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nse1342.tmp	success or wait	1	4035BF	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsp1382.tmp	success or wait	1	4058EE	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xavbedcnsrtbhix	unknown	11781	74 44 2a 40 4a de 03 70 b3 09 87 00 0b 8d 9e 9d ab 0c 9e b7 3e 61 e0 b0 e5 b4 ae 65 f4 84 36 71 fc 8c 7b c2 72 fc 77 ca 7a 8a 86 45 d4 4c 53 9a 2c 5f 4e df 04 a1 8e f2 9a a4 9e ef f9 c2 f0 5f c1 f0 24 10 be b5 7f 78 d7 21 23 cc 18 6c da 91 9b 50 33 2d 2f d8 22 78 26 de e8 58 ff 09 0b 34 22 54 02 fa c4 b0 1b 15 17 00 5e a0 0e c6 d0 b8 67 71 73 1c 0c bc 6a 22 2c 90 43 3d 3f 68 66 88 76 2e 38 d7 4f 59 5b 44 ac e3 52 0a 14 2f ab a5 a7 50 b0 ef 9e 16 60 37 b7 81 83 ac b2 cb ba 72 7c 0f 93 8d 8f b8 ae d7 86 3e 48 17 e0 ea ec 94 05 33 e1 5a a4 6f fc f6 f8 df e7 ff ed a6 b0 77 c8 d2 d4 fb d9 1b c9 82 8c 4f 24 1e 20 c7 cf 67 d5 8e 98 17 30 3a 3c 4d b2 27 df f1 6d 0a 0c 06 2d 69 4d 03 fb 3d f5 03 01 a3 11 c9 53 c7 11 ff b1 17 cf a1 d1 17 4b b7 65 1d a7 23 65 b5 85	tD*@J..p.....>a.....e.. 6q..{.r.w.z..E.LS.,_N..... ..._..$....x.!#..l...P3-/."x&. .X...4"T.....^.....gqs...j" ,.C=? hf.v.8.OY[D..R../...P.... `7.....r|.....>H.....3.Z .o.....w.....O$. ..g....0: <M.'..m...-iM..=.....S... .....K.e..#e..	success or wait	1	405D51	WriteFile
C:\Users\user\AppData\Local\Temp\nejus0or2e4wbg8rhay	unknown	32768	fa 5c 85 35 c1 06 e8 b7 78 29 06 b7 12 e5 10 62 3f ad bd ba 6b ad 31 50 26 e0 aa 0f 12 c5 da a7 82 a0 e6 66 9a 70 91 10 83 33 ba fd 64 b8 3b 9f 76 52 37 db 50 bd fb 99 63 0a a1 9a a8 31 d8 8a b9 b2 75 19 61 48 dc 19 80 68 53 45 7d aa ac 08 5e 26 ce 40 77 4c e3 c1 44 49 bb 8b 97 de bd 04 c9 04 16 ab 49 ef a2 60 56 53 e7 ef 76 b3 ef 4a 86 92 2a 6f 7f 41 d7 ea 0d 40 ff 97 5c 0f f8 53 23 91 1e 61 55 20 af 87 a2 a4 25 9a 97 1a b4 de f0 21 49 9a a6 83 59 6d dd 56 bf a6 a8 d2 b7 23 d3 c7 72 36 d8 1b 6f da 0b 59 62 41 99 62 4e 0a e9 0a e2 2f 00 0f 1c bc b6 73 6a 8e 54 81 8c 45 58 1d 2e 47 05 8d 1d 46 1b fa f9 6b 47 92 7d 37 23 36 78 81 1f b6 83 3c 05 7d 16 93 01 f8 ae f0 4c d8 18 4b ac 44 85 e7 a5 b3 48 fb 23 61 05 b0 d8 7e 3a 5f fb 27 8e ea dd e5 87 e6 15 c8 df	.\.5....x).....b?...k.1P&..... .....f.p...3..d.;.vR7.P...c... .1....u.aH...hSE}...^&.@wL. .DI.....I..`VS..v..J..*o.A.. .@..\..S#..aU ....%.....!I... Ym.V.....#..r6..o..YbA.bN... ./ .....sj.T..EX..G...F...kG.}7# 6x....<.}.....L..K.D....H.#a.. .~:_.'.....	success or wait	9	405D51	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsp1382.tmp\xktfu.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 3e 92 66 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0e 10 00 04 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............................ ....PE..L...>.f`.... ....!.......	success or wait	1	405D51	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	512	success or wait	794	405D22	ReadFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	4	success or wait	2	405D22	ReadFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	4	success or wait	14	405D22	ReadFile
C:\Users\user\AppData\Local\Temp\xavbedcnsrtbhix	unknown	11781	success or wait	1	10001221	ReadFile
C:\Users\user\AppData\Local\Temp\nejus0or2e4wbg8rhay	unknown	283136	success or wait	1	28520B5	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	285085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	285085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	285085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	285085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	285085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	285085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	285085D	ReadFile

Analysis Process: dhcpmon.exe PID: 6816 Parent PID: 6600

General

Start time:	17:21:31
Start date:	08/04/2021
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:	702907 bytes
MD5 hash:	F72A7FD231E50F9B43C3DAB470364846
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.323797763.0000000002561000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.323934536.0000000003561000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.323934536.0000000003561000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.323934536.0000000003561000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.326163063.0000000004A62000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.326163063.0000000004A62000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.326163063.0000000004A62000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.323984965.000000000359C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.323984965.000000000359C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.323578165.00000000024C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000011.00000002.323578165.00000000024C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.323578165.00000000024C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.323578165.00000000024C0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.322836165.000000000050C000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.322836165.000000000050C000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.322836165.000000000050C000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.323888903.00000000025B0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.322659318.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000011.00000002.322659318.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.322659318.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.322659318.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCFCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCFCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E00C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E00C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C9B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C9B1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: 6212 Parent PID: 6752

General

Start time:	17:21:42
Start date:	08/04/2021

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:	702907 bytes
MD5 hash:	F72A7FD231E50F9B43C3DAB470364846
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: 00000016.00000001.319250838.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000001.319250838.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000001.319250838.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.338981000.00000000023B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000016.00000002.338981000.00000000023B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.338981000.00000000023B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.338981000.00000000023B0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.339113549.0000000002432000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.339113549.0000000002432000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.339113549.0000000002432000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.339334436.00000000034CC000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.339334436.00000000034CC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.339271124.00000000024E0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.339201684.0000000002491000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.339302702.0000000003491000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.339302702.0000000003491000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.339302702.0000000003491000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.338373270.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000016.00000002.338373270.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.338373270.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.338373270.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.338595453.00000000005A8000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.338595453.00000000005A8000.00000004.00000020.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.338595453.00000000005A8000.00000004.00000020.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCFCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCFCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C9B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C9B1B4F	ReadFile

Disassembly

Code Analysis