ID: 452188
Sample Name:
gXcRJ8123G.exe
Cookbook: default.jbs
Time: 23:02:13
Date: 21/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

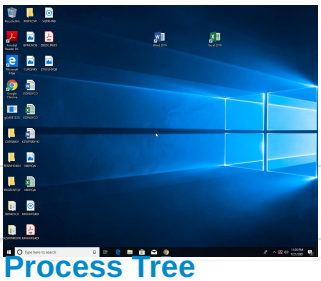
Windows Analysis Report gXcRJ8123G.exe

Overview

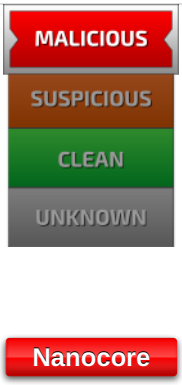
General Information

Sample Name:	gXcRJ8123G.exe
Analysis ID:	452188
MD5:	767e1c497ff0d61..
SHA1:	118e1e764cd05b..
SHA256:	f84b3abd9e10ed3.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



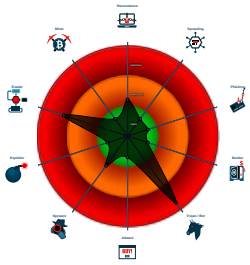
Nanocore

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- gXcRJ8123G.exe (PID: 1700 cmdline: 'C:\Users\user\Desktop\gXcRJ8123G.exe' MD5: 767E1C497FF0D617DE66C2D8ECE44C49)
  - schtasks.exe (PID: 6092 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp28BF.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2576 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4108 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp2C3B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- gXcRJ8123G.exe (PID: 1872 cmdline: C:\Users\user\Desktop\gXcRJ8123G.exe 0 MD5: 767E1C497FF0D617DE66C2D8ECE44C49)
- dhcpmon.exe (PID: 2944 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 767E1C497FF0D617DE66C2D8ECE44C49)
- dhcpmon.exe (PID: 5700 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 767E1C497FF0D617DE66C2D8ECE44C49)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "03e670ce-e449-4fbc-8c90-b68dc609",
  "Group": "Scammer",
  "Domain1": "188.141.118.122",
  "Domain2": "188.141.118.122",
  "Port": 6666,
  "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

Initial Sample

Source	Rule	Description	Author	Strings
gXcRJ8123G.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
gXcRJ8123G.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
gXcRJ8123G.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
gXcRJ8123G.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q

Copyright Joe Security LLC 2021

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000000.352570827.000000000782000.00000002.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000007.00000000.352570827.000000000782000.00000002.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000007.00000000.352570827.000000000782000.00000002.00020000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000006.00000002.348559232.000000000298000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
00000006.00000002.348559232.000000000298 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x23ba3:$a: NanoCore • 0x23bfc:$a: NanoCore • 0x23c39:$a: NanoCore • 0x23cb2:$a: NanoCore • 0x23c05:$b: ClientPlugin • 0x23c42:$b: ClientPlugin • 0x24540:$b: ClientPlugin • 0x2454d:$b: ClientPlugin • 0x1b919:$e: KeepAlive • 0x2408d:$g: LogClientMessage • 0x2400d:$i: get_Connected • 0x15bd5:$j: #=q • 0x15c05:$j: #=q • 0x15c41:$j: #=q • 0x15c69:$j: #=q • 0x15c99:$j: #=q • 0x15cc9:$j: #=q • 0x15cf9:$j: #=q • 0x15d29:$j: #=q • 0x15d45:$j: #=q • 0x15d75:$j: #=q
Click to see the 41 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.gXcRJ8123G.exe.420dc45.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x605:$x1: NanoCore.ClientPluginHost • 0x3bd6:$x1: NanoCore.ClientPluginHost • 0x63e:$x2: IClientNetworkHost
0.3.gXcRJ8123G.exe.420dc45.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x605:$x2: NanoCore.ClientPluginHost • 0x3bd6:$x2: NanoCore.ClientPluginHost • 0x720:$s4: PipeCreated • 0x3cb4:$s4: PipeCreated • 0x61f:$s5: IClientLoggingHost • 0x3bf0:$s5: IClientLoggingHost
5.2.gXcRJ8123G.exe.36930ed.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x24170:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x2419d:$x2: IClientNetworkHost
5.2.gXcRJ8123G.exe.36930ed.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0x24170:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0x2524b:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost • 0x2418a:$s5: IClientLoggingHost
5.2.gXcRJ8123G.exe.36930ed.2.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 75 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Networking:

- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- .NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Stealing of Sensitive Information:

- Yara detected Nanocore RAT

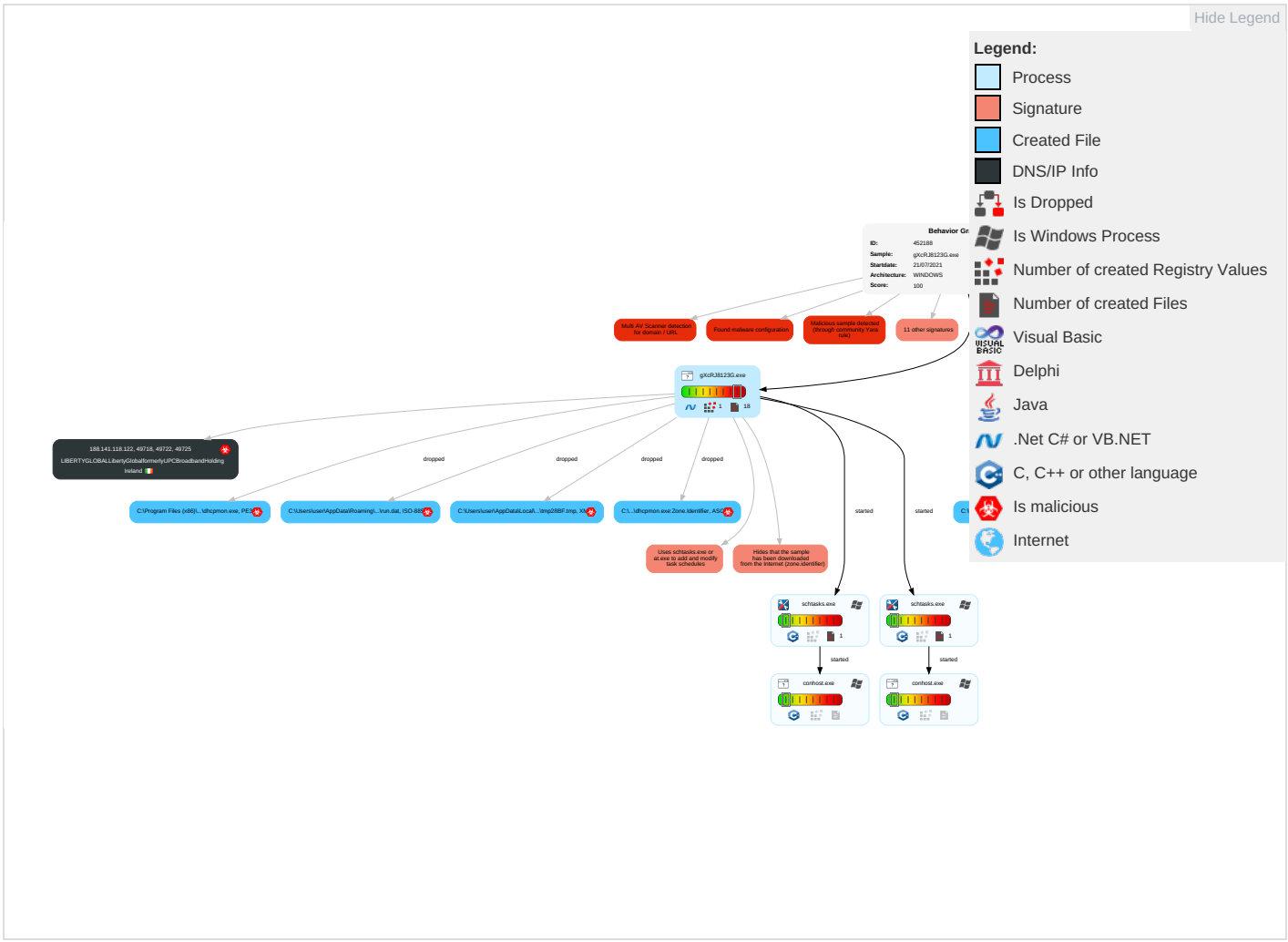
Remote Access Functionality:

- 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	Netw Effe
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 2	Masquerading 2	Input Capture 1 1	Query Registry 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavd Inse Netv Com
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Expl Red Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Man Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Den Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acce

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
gXcRJ8123G.exe	84%	Virustotal		Browse
gXcRJ8123G.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
gXcRJ8123G.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
gXcRJ8123G.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	84%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.gXcRJ8123G.exe.60000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.dhcpmon.exe.780000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.gXcRJ8123G.exe.60000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.2.dhcpmon.exe.390000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.0.gXcRJ8123G.exe.640000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.0.dhcpmon.exe.390000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.dhcpmon.exe.780000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
188.141.118.122	6%	Virustotal		Browse
188.141.118.122	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
188.141.118.122	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.141.118.122	unknown	Ireland		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452188
Start date:	21.07.2021
Start time:	23:02:13
Joe Sandbox Product:	CloudBasic

Copyright Joe Security LLC 2021

Overall analysis duration:	0h 9m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	gXcRJ8123G.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:	23
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@10/12@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
23:03:05	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\gXcRJ8123G.exe" s>$(Arg0)
23:03:05	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
23:03:05	API Interceptor	1032x Sleep call for process: gXcRJ8123G.exe modified
23:03:07	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LIBERTYGLOBALLibertyGlobalformerly UPCBroadbandHolding	xjYvqOne1t	Get hash	malicious	Browse	• 31.5.149.216
	iUmNR6tkEd	Get hash	malicious	Browse	• 178.202.206.19
	eAtDhymLzp	Get hash	malicious	Browse	• 213.93.27.100
	ehn0f1d63M	Get hash	malicious	Browse	• 213.126.201.232
	zhPAQB7FPV	Get hash	malicious	Browse	• 145.252.248.205

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	wy2BysBF1U	Get hash	malicious	Browse	• 86.49.148.244
	jhUxzb7jPW	Get hash	malicious	Browse	• 91.119.249.10
	dFwIxBbz2d	Get hash	malicious	Browse	• 89.101.120.139
	7f8BlPBZMS	Get hash	malicious	Browse	• 213.126.148.27
	9bCnBwR693.exe	Get hash	malicious	Browse	• 78.45.53.24
	nRjbMQ5Jua.exe	Get hash	malicious	Browse	• 84.117.126.143
	Vk3A1yJJMg	Get hash	malicious	Browse	• 83.103.130.246
	rnQYDw7A4G	Get hash	malicious	Browse	• 95.76.74.163
	Af1Fnq4I4G	Get hash	malicious	Browse	• 88.146.165.84
	395d6gwkWK	Get hash	malicious	Browse	• 213.126.20 1.255
	wZ6O9wSQ4e	Get hash	malicious	Browse	• 86.49.196.177
	b8oaj84zgz	Get hash	malicious	Browse	• 77.251.162.101
	eubqHHIQkc	Get hash	malicious	Browse	• 88.153.34.82
	popsmoke.mpsl	Get hash	malicious	Browse	• 62.195.46.186
	popsmoke.mpsl	Get hash	malicious	Browse	• 62.143.241.216

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\gXcRJ8123G.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207872
Entropy (8bit):	7.450095771993313
Encrypted:	false
SSDEEP:	6144:sLV6Bta6dtJmakIM5KcGLYiO5C3e6s7338vSa:sLV6BtpmkjYiOS1k3Ta
MD5:	767E1C497FF0D617DE66C2D8ECE44C49
SHA1:	118E1E764CD05B98C631BB9A5687ACAE94F208E1
SHA-256:	F84B3ABD9E10ED3595FB957BA10F2C222FA6AC99605BBFD768CC65EE4F59E6E8
SHA-512:	F24ACF37C91C0FBFB02C17566D5B9D3FF548BD414D11F343AB56B4105D257721FC54C57254D3078AE30D4EC54D403EB5AF3E50A648B4B1F8C579D745F50B492
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 84%, Browse • Antivirus: ReversingLabs, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....b..... .....@.. ....8...W.... ..._..... ....H.....text..... ....`.reloc.....@..B.rsrc...._... ...`.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s 8....-&&s9....,$&s:.....s;.....*.....+.....+....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$..... ~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

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

Process:	C:\Users\user\Desktop\gXcRJ8123G.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

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
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_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\gXcRJ8123G.exe.log	
Process:	C:\Users\user\Desktop\gXcRJ8123G.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp28BF.tmp	
Process:	C:\Users\user\Desktop\gXcRJ8123G.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1303
Entropy (8bit):	5.115734872180681
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0V5lxtn:cbk4oL600QydbQxIYODOLedq3kj
MD5:	447A6AD04F7E1B9672E3B07786B1524A
SHA1:	043FAD6383FA97E1E4BCD0917B113EDAF35550C9
SHA-256:	55F70B35DB53C7218954340D87AFB1EDC889BE378C0327036BF947251A361AEB
SHA-512:	2546986CD9D35408C2D89834711E40129A4C8EAB75BC5A1C4051B68CB27446D60CAA19A0F1C5EB1421B6F4495E20A4CC1F96CF9446625E15424A7C293B173A0
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp2C3B.tmp	
Process:	C:\Users\user\Desktop\gXcRJ8123G.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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\gXcRJ8123G.exe
File Type:	data
Category:	dropped
Size (bytes):	1736
Entropy (8bit):	7.094528505897445
Encrypted:	false
SSDEEP:	48:Ik/t3FmH8Uk/t3FmH8Uk/t3FmH8Uk/t3FmH8Uk/t3FmH8Uk/t3FmH8Uk/t3FmH8L:ft3Ucrt3Ucrt3Ucrt3Ucrt3Ucrt3Ucr9
MD5:	C9A901CEF4675F82D1F8407B7E1DA172
SHA1:	03480F0CAFD5689E41D7509DF92AE700B78D1693
SHA-256:	61488189C23B604117304C41F02C5E722985D264CCAC36D3DFA0589C8D5AD1C7
SHA-512:	8A02A9BF579D8C1464C4245AB21836604878E90B4EDEFCDE5A8D5D25872FC1DCE1CB82D72C9406DC24DE6CC1982C9A8204CAA798CD8BF06D47EBA600968659
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL....f.Z#.|...@HkG....G..O*V.....pz...."....r...w&&|..c..3}~.....~...os..f.....4..1.gJ.'.d".L...A.t...F.{....C.|&.wGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL....f.Z#.|...@HkG....G..O*V.....pz...."...r...w&&|..c..3}~.....~...os..f.....4..1.gJ.'.d".L...A.t...F.{....C.|&.wGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL....f.Z#.|...@HkG....G..O*V.....pz...."....r...w&&|..c..3}~.....~...os..f.....4..1.gJ.'.d".L...A.t...F.{....C.|&.wGj.h\.3.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\gXcRJ8123G.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:qF8t:q6
MD5:	AB1EF4A9F831D79EE720D72C90642ECE
SHA1:	9246DF20EE6CEBB1852A3774A7ED42A17ED8EEF0
SHA-256:	0305722508F8C58572086CD7F3718E2382D189EA7FF6020283354FEB9F110DCC
SHA-512:	058DFE6F015846BB70F6DF9E5C17CA4958C0202DC98283ABE0105236AC2A316A6547A09D1A725FE35008CE4C42099F6C8D5726E2867166C90A2BB312B32D7541
Malicious:	**true**
Preview:	...].L.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\Desktop\gXcRJ8123G.exe
File Type:	data
Category:	modified
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
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\gXcRJ8123G.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYVsRLY6oRDT6P2bfVn1: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\gXcRJ8123G.exe
File Type:	data
Category:	dropped
Size (bytes):	433688
Entropy (8bit):	**7.999519077450246**
Encrypted:	**true**
SSDEEP:	12288:dcRKtiKlC1FGhWjoORvi5oCILR9Eax5uoj:KRCiKECCGoD9Eaioj
MD5:	D2D87B1E9F691E38698A9683C9E213C1
SHA1:	87FAA25A212348CCD20567929D52A0ADE5BE07CE
SHA-256:	4115C31136A8A8F4642D3F5E7032A248381FCF36B047CFD911F974600F140039
SHA-512:	541F3C4C9CA97C085065FA5881D9A336F0BE474C90D1C65379CA7CB7F084B6496ED52A61F9133FD29DE5DB57C2B1F2CC302498579C5A158F823612EAC248C5D
Malicious:	false
Preview:	.....O.....\8..5N..`S.]..[r.$*>.\.#v&..$.....Z.i..M.Mn5.@..@...3.R..Y...}>C.b....Z.....K..^.d...Z...K.#...dn$e ..XP.^.#.....V...dB.Kn.Y.c..-k....M.D...Q.S..R.X....._...Zz...#.=<.V.NHZq.h..ON..oq.:...,7H...../..Q..R.u6.."....<.`..z.5b($..9.CF.F1...o?.h.}....;Ay....kL}7...I.-.}..D&...C....%.J..+..1.5.a..Ih....s.....G..?..9^0e...p..FCvNt.e...B/...y.h.G.0..o,Q.2[.....e.P8.....yr...*..Q..*..../..S..m.....\.wA.a1.]...oW.....PY..h....f:....Ss.....\.8...@R._A...M..X....V.f).]z..u{.z-....W...NaT+.&:...1.D../.7..\.S..z..!.....#..F.d.....*.m'.....6.2....:H...bd]..._.....}.n.=...I.7%r.>...B.Q.K..q...Ex.6.6....P..^...i...Mx...;g...,t..fCd.\.b....e{.\...Y=4.....+..T....j}..|66g.s...z...Y.kTi..?Xy...5\...SO..W.U.3A.$.I..{.D...no.E..v.2.:..a..hdhO..t.w.k..T|Po.....D?..mG.[.2.;....+...8.6.h!..w.3...w.o.....|....f.v.to.B.{`o..a.....f.cu.....?....."...u..EA...^)W..z..jtU{^.....5#....y.s.....e.l..&...%...

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\gXcRJ8123G.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	40
Entropy (8bit):	4.361768795973195
Encrypted:	false
SSDEEP:	3:oNN2+WCkf+0Cn:oNN2RCf0C
MD5:	57727D13BAD31F90F435367844801B81
SHA1:	BCE921899C2A359675AE9ACF8AA9C7181A03EA20
SHA-256:	ABC4C5E92B977739708223B5A0EE20A2898D3065997A991094C2360654B4EF8F
SHA-512:	FFCD3E598E062EF47F3087E3956E2A3C2DB02B1CE32463D9665FFC458C5C3D9EF1394BC8852733C258FE4592B7ED2CC600E7BF6FB716AE9A6A39C645B06ED67
Malicious:	false
Preview:	C:\Users\user\Desktop\gXcRJ8123G.exe

Static File Info

General

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.450095771993313
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	gXcRJ8123G.exe
File size:	207872
MD5:	767e1c497ff0d617de66c2d8ece44c49
SHA1:	118e1e764cd05b98c631bb9a5687acae94f208e1
SHA256:	f84b3abd9e10ed3595fb957ba10f2c222fa6ac99605bbfd768cc65ee4f59e6e8
SHA512:	f24acf37c91c0fbfb02c17566d5b9d3ff548bd414d11f343ab56b4105d257721fc54c57254d3078ae30d4ec54d403eb5af3e50a648b4b1f8c579d745f50b492c
SSDEEP:	6144:sLV6Bta6dtJmakIM5KcGLYiO5C3e6s7338vSa:sLV6BtpmkjYiOS1k3Ta
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....b..... .....@.. ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41e792
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x54E927A1 [Sun Feb 22 00:49:37 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1c798	0x1c800	False	0.594512404057	data	6.59805438752	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x22000	0x15fc8	0x16000	False	1.00026633523	data	7.99757268531	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Network Behavior

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: gXcRJ8123G.exe PID: 1700 Parent PID: 5768

General

Start time:	23:03:02
Start date:	21/07/2021
Path:	C:\Users\user\Desktop\gXcRJ8123G.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\gXcRJ8123G.exe'
Imagebase:	0x640000
File size:	207872 bytes
MD5 hash:	767E1C497FF0D617DE66C2D8ECE44C49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000000.00000003.335010168.00000000041EB000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000000.324690560.0000000000642000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.324690560.0000000000642000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.324690560.0000000000642000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 6092 Parent PID: 1700

General

Start time:	23:03:03
Start date:	21/07/2021
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\tmp28BF.tmp'
Imagebase:	0x1030000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 2576 Parent PID: 6092

General

Start time:	23:03:03
Start date:	21/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 4108 Parent PID: 1700

General

Start time:	23:03:04
Start date:	21/07/2021
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\tmp2C3B.tmp'
Imagebase:	0x1030000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 3700 Parent PID: 4108

General

Start time:	23:03:04
Start date:	21/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: gXcRJ8123G.exe PID: 1872 Parent PID: 936

General

Start time:	23:03:05
Start date:	21/07/2021
Path:	C:\Users\user\Desktop\gXcRJ8123G.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\gXcRJ8123G.exe 0
Imagebase:	0x60000
File size:	207872 bytes
MD5 hash:	767E1C497FF0D617DE66C2D8ECE44C49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.345462814.0000000000062000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.345462814.0000000000062000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.345462814.0000000000062000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.331597446.0000000000062000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.331597446.0000000000062000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.331597446.0000000000062000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.346411950.0000000002641000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.346411950.0000000002641000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.346446290.0000000003641000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.346446290.0000000003641000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 2944 Parent PID: 936

General

Start time:	23:03:05
Start date:	21/07/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x7ff614b90000
File size:	207872 bytes
MD5 hash:	767E1C497FF0D617DE66C2D8ECE44C49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.348559232.0000000002981000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.348559232.0000000002981000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.346521938.0000000000392000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.346521938.0000000000392000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.346521938.0000000000392000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.348658355.0000000003981000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.348658355.0000000003981000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000000.332506578.0000000000392000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000000.332506578.0000000000392000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000000.332506578.0000000000392000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 84%, Virustotal, Browse • Detection: 100%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 5700 Parent PID: 3440

General

Start time:	23:03:15
Start date:	21/07/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x780000
File size:	207872 bytes
MD5 hash:	767E1C497FF0D617DE66C2D8ECE44C49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.352570827.0000000000782000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.352570827.0000000000782000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.352570827.0000000000782000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.368916384.0000000003E71000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.368916384.0000000003E71000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.368877575.0000000002E71000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.368877575.0000000002E71000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.367686754.0000000000782000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.367686754.0000000000782000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.367686754.0000000000782000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021