ID: 508792
Sample Name: doa8GHSloq
Cookbook: default.jbs
Time: 16:09:38
Date: 25/10/2021
Version: 33.0.0 White Diamond

Table of Contents

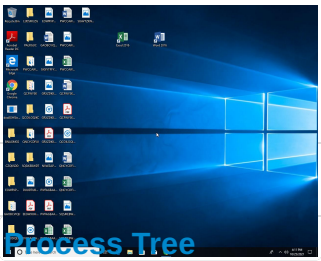
Windows Analysis Report doa8GHSloq

Overview

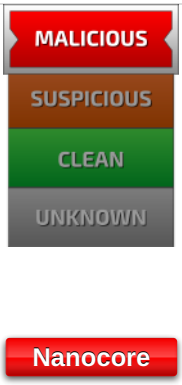
General Information

Sample Name:	doa8GHSloq (renamed file extension from none to exe)
Analysis ID:	508792
MD5:	f85ca66e06121eb.
SHA1:	141bc2598b79d8..
SHA256:	2483d6141d48f38.
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection

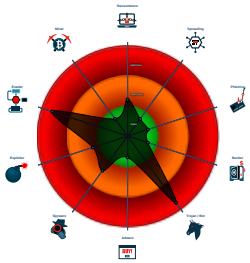


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…

Classification



- **System is w10x64**
- doa8GHSloq.exe (PID: 6672 cmdline: 'C:\Users\user\Desktop\doa8GHSloq.exe' MD5: F85CA66E06121EB29B26D78CC3F64554)
  - doa8GHSloq.exe (PID: 7164 cmdline: C:\Users\user\Desktop\doa8GHSloq.exe MD5: F85CA66E06121EB29B26D78CC3F64554)
  - doa8GHSloq.exe (PID: 4820 cmdline: C:\Users\user\Desktop\doa8GHSloq.exe MD5: F85CA66E06121EB29B26D78CC3F64554)
    - schtasks.exe (PID: 3180 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpA5BD.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 3912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5700 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpAC94.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4248 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- doa8GHSloq.exe (PID: 3860 cmdline: C:\Users\user\Desktop\doa8GHSloq.exe 0 MD5: F85CA66E06121EB29B26D78CC3F64554)
  - doa8GHSloq.exe (PID: 5356 cmdline: C:\Users\user\Desktop\doa8GHSloq.exe MD5: F85CA66E06121EB29B26D78CC3F64554)
- dhcpmon.exe (PID: 6268 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: F85CA66E06121EB29B26D78CC3F64554)
  - dhcpmon.exe (PID: 6528 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: F85CA66E06121EB29B26D78CC3F64554)
- dhcpmon.exe (PID: 6520 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: F85CA66E06121EB29B26D78CC3F64554)
  - dhcpmon.exe (PID: 4140 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: F85CA66E06121EB29B26D78CC3F64554)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "b4ede67b-be7e-44fd-9e96-0c0f6d15",
  "Group": "Default",
  "Domain1": "watermalon1.sytes.net",
  "Domain2": "",
  "Port": 2010,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH|"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.332763752.00000000045F1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x32b8ad:$x1: NanoCore.ClientPluginHost • 0x35e2cd:$x1: NanoCore.ClientPluginHost • 0x32b8ea:$x2: IClientNetworkHost • 0x35e30a:$x2: IClientNetworkHost • 0x32f41d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x361e3d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000010.00000002.332763752.00000000045F1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000010.00000002.332763752.00000000045F1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x32b615:$a: NanoCore • 0x32b625:$a: NanoCore • 0x32b859:$a: NanoCore • 0x32b86d:$a: NanoCore • 0x32b8ad:$a: NanoCore • 0x35e035:$a: NanoCore • 0x35e045:$a: NanoCore • 0x35e279:$a: NanoCore • 0x35e28d:$a: NanoCore • 0x35e2cd:$a: NanoCore • 0x32b674:$b: ClientPlugin • 0x32b876:$b: ClientPlugin • 0x32b8b6:$b: ClientPlugin • 0x35e094:$b: ClientPlugin • 0x35e296:$b: ClientPlugin • 0x35e2d6:$b: ClientPlugin • 0xba19d:$c: ProjectData • 0x2947cd:$c: ProjectData • 0x32b79b:$c: ProjectData • 0x35e1bb:$c: ProjectData • 0x32c1a2:$d: DESCrypto
00000014.00000002.337336999.00000000029B1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000003.360949669.000000000421 4000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1e62:$a: NanoCore • 0x1e87:$a: NanoCore • 0x1ee0:$a: NanoCore • 0x1207d:$a: NanoCore • 0x120a3:$a: NanoCore • 0x120ff:$a: NanoCore • 0x1ef54:$a: NanoCore • 0x1efad:$a: NanoCore • 0x1efe0:$a: NanoCore • 0x1f20c:$a: NanoCore • 0x1f288:$a: NanoCore • 0x1f8a1:$a: NanoCore • 0x1f9ea:$a: NanoCore • 0x1febe:$a: NanoCore • 0x201a5:$a: NanoCore • 0x201bc:$a: NanoCore • 0x2575a:$a: NanoCore • 0x257d4:$a: NanoCore • 0x2a371:$a: NanoCore • 0x2b72b:$a: NanoCore • 0x2b775:$a: NanoCore
Click to see the 47 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
21.2.dhcpmon.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
21.2.dhcpmon.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
21.2.dhcpmon.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
21.2.dhcpmon.exe.400000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
19.2.dhcpmon.exe.423eac4.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 125 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.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)

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

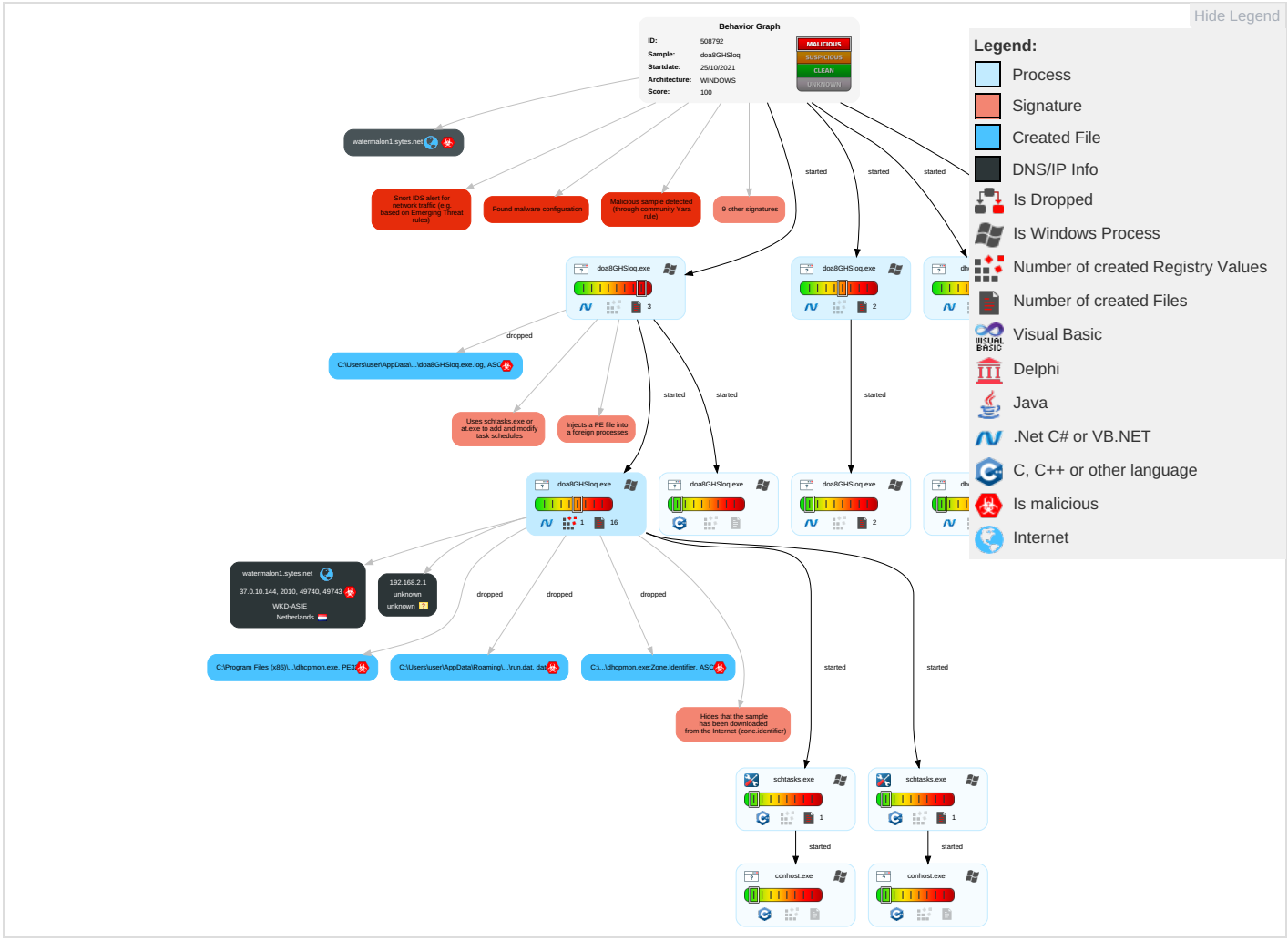
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 2	Input Capture 2 1	Security Software Discovery 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

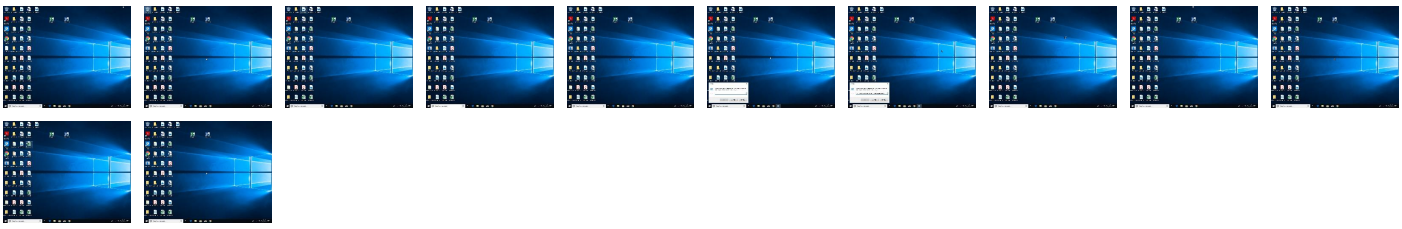
Behavior Graph



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
doa8GHSloq.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
19.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
18.2.doa8GHSloq.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com8	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/M	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/tali	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/~	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmFwaQ	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
watermalon1.sytes.net	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/h	0%	URL Reputation	safe	
http://www.carterandcone.comold	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.carterandcone.comTC.	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/&	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/fi-fZ	0%	Avira URL Cloud	safe	
http://www.tiro.comw	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/S	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0et	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.fontbureau.comS	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/M	0%	URL Reputation	safe	
http://www.fontbureau.comdw	0%	Avira URL Cloud	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.sajatypeworks.comauT	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/w	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/?	0%	URL Reputation	safe	
http://www.carterandcone.comn-uB	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.comdh	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/w	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.tiro.comY	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/h	0%	URL Reputation	safe	
http://www.tiro.comslnt8	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/d	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
watermalon1.sytes.net	37.0.10.144	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
watermalon1.sytes.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.0.10.144	watermalon1.sytes.net	Netherlands		198301	WKD-ASIE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	508792
Start date:	25.10.2021
Start time:	16:09:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	doa8GHSloq (renamed file extension from none to 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:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@20/9@20/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14% (good quality ratio 9.1%) • Quality average: 40.7% • Quality standard deviation: 36.1%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:10:40	API Interceptor	871x Sleep call for process: doa8GHSloq.exe modified
16:10:44	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
16:10:47	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\doa8GHSloq.exe" s>$(Arg0)
16:10:49	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
16:10:52	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
watermalon1.sytes.net	EDG.exe	Get hash	malicious	Browse	• 103.125.189.85

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WKD-ASIE	OPEN_2021-10-25_09-58.exe	Get hash	malicious	Browse	• 37.0.10.118
	CV.exe	Get hash	malicious	Browse	• 37.0.10.22
	Debitnote-s3update.exe	Get hash	malicious	Browse	• 37.0.10.22
	SKypfeGItc.exe	Get hash	malicious	Browse	• 37.0.10.190
	Purchase Order.exe	Get hash	malicious	Browse	• 37.0.10.22
	HBC.exe	Get hash	malicious	Browse	• 37.0.10.15
	85QKQNr7mm.xlsx	Get hash	malicious	Browse	• 37.0.10.15
	AB948F038175411DC326A1AAD83DF48D6B656325 01551.exe	Get hash	malicious	Browse	• 37.0.8.235
	FC2E04D392AB5E508FDF6C90CE456BFD0AF6DEF1 F10A2.exe	Get hash	malicious	Browse	• 37.0.10.214
	3qZB2fO4lG.exe	Get hash	malicious	Browse	• 37.0.8.193
	365F984ABE68DDD398D7B749FB0E69B0F29DAF86 F0E3E.exe	Get hash	malicious	Browse	• 37.0.11.8
	CQUOTATION REQUEST4.scr.exe	Get hash	malicious	Browse	• 37.0.10.252
	gy6JsH7kJx.exe	Get hash	malicious	Browse	• 37.0.10.225
	About company.doc	Get hash	malicious	Browse	• 37.0.10.225
	SecuriteInfo.com.Virus.Win32.Save.a.26327.exe	Get hash	malicious	Browse	• 37.0.10.225
	ifCgoV9Ykq.exe	Get hash	malicious	Browse	• 37.0.10.225
	Agent_UDPRat.exe	Get hash	malicious	Browse	• 37.0.11.171
	Agent_UDPRat.exe	Get hash	malicious	Browse	• 37.0.11.171
	Order.exe	Get hash	malicious	Browse	• 37.0.10.22
	Order.exe	Get hash	malicious	Browse	• 37.0.10.22

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\doa8GHSloq.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	823808
Entropy (8bit):	7.825510973865646
Encrypted:	false
SSDEEP:	12288:JANTdXQBp9LbKV16MeEDyW89RQWQgZ8Wd9f8RWcz+nXUJHP4m9XQ6+0/l:iTdXQBjSeEDyWwLQO39URWL
MD5:	F85CA66E06121EB29B26D78CC3F64554
SHA1:	141BC2598B79D80BB3CEDA6FE98C49AB7C694DD8
SHA-256:	2483D6141D48F387AAD22F1BEC5C45945BCA933EB35BA13D6FF65A46B8720885
SHA-512:	53A9CAAD2DF5549538085EBAE5427634B841398FC794502FD0B3D6E3F39313D1A738C34EC95AD47F4B37C61045B8E04CDD3339EED6EDEEB5C0F91ED7C4E56FD7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ua..... .....@.. ....@.....d...W..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....0...4.....`.....!3.,...&.z..+...AC.w.h-..B.$.57/1.G.1.^E..S.bn.vC.u...wH.s.....bN!U.|..:..0.>..l.J.5f.G..D..r. ...1.....M.B.....K.....|=.,..g...1.b.....v..V?.....O..}.dz.\....A.l0...H.....G...9V6p.c...Z.....Fo..}..kN....1..m..T.....Se%\".wC(a..M..V.W.H.....z,...D.J..F..q.....1.Cb.#.e.0,..B8. F02.....q+.x.#.]..0.H..w..=s..<...o'.Y.U..9@.v{...k..FE%]:.~...bd...Yc.....U.a

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\doa8GHSloq.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:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Reputation:	unknown
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\doa8GHSloq.exe.log	
Process:	C:\Users\user\Desktop\doa8GHSloq.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\doa8GHSloq.exe.log	
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	unknown
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\tmpAC94.tmp	
Process:	C:\Users\user\Desktop\doa8GHSloq.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
Reputation:	unknown
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\doa8GHSloq.exe
File Type:	data
Category:	modified
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356A5
Malicious:	false
Reputation:	unknown
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.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\doa8GHSloq.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:I8:I8
MD5:	E17438243D171CBD003AEF62A1CB4247
SHA1:	98F4323EDEAD9F3D1B8915669A7D782C620DF4DB
SHA-256:	A9A86D410BCD1CDC68D150F01C9EBD89687F43493C9B43731119DF01741DFF77

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SHA-512:	6E91CE19E77F1463A4A8F3634F0D6B360BCD51EC4767FB5F982C7BA38CB8D2B19B93F03C039DACF39D869D9673D7B68BBBB9B26F486807D09B7E965AB0CA293
Malicious:	**true**
Reputation:	unknown
Preview:	.....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\doa8GHSloq.exe
File Type:	data
Category:	dropped
Size (bytes):	426840
Entropy (8bit):	**7.999608491116724**
Encrypted:	**true**
SSDEEP:	12288:zKf137EiDsTjevgA4p0V7njXuWSvdVU7V4OC0Rr:+134i2lp67i5d8+OCg
MD5:	963D5E2C9C0008DFF05518B47C367A7F
SHA1:	C183D601FABBC9AC8FBFA0A0937DECC677535E74
SHA-256:	5EACF2974C9BB2C2E24CDC651C4840DD6F4B76A98F0E85E90279F1DBB2E6F3C0
SHA-512:	0C04E1C1A13070D48728D9F7F300D9B26DEC6EC8875D8D3017EAD52B9EE5BDF9B651A7F0FCC537761212831107646ED72B8ED017E7477E600BC0137EF857AE2
Malicious:	false
Reputation:	unknown
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^.._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m...RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:...L.g<.....I..%4[.G^.~.I'.....v.p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...".bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&....g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\doa8GHSloq.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.357837824971466
Encrypted:	false
SSDEEP:	3:oNWXp5vBK4JP0C:oNWXpF8EsC
MD5:	2EBF6D6EA84DE2782525A8EF80DCE065
SHA1:	5621AD39CB47B3E548BBC07CBD04D292D2C2AF46
SHA-256:	874B80E173A64CC41894A257147983666F52EB467E6DE3ED535A6A95D31A1EB8
SHA-512:	E96E402132CA8C0059CDE12ED7D3FFEF3F471C3D71AC7A224D28A8C7ADF48A1815321C73B93AB1858146E58EC8722209EDAFF8668A0F3581885C82CF4AE2AA8A
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\doa8GHSloq.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.825510973865646
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	doa8GHSloq.exe
File size:	823808
MD5:	f85ca66e06121eb29b26d78cc3f64554
SHA1:	141bc2598b79d80bb3ceda6fe98c49ab7c694dd8
SHA256:	2483d6141d48f387aad22f1bec5c45945bca933eb35ba13d6ff65a46b8720885

General

SHA512:	53a9caad2df5549538085ebae5427634b841398fc794502fd0b3d6e3f39313d1a738c34ec95ad47f4b37c61045b8e04cdd3339eed6edeeb5c0f91ed7c4e56fd7
SSDEEP:	12288:JANTdXQBp9LbKV16MeEDyW89RQWQgZ8Wd9f8RWcz+nXUJHP4m9XQ6+0/l:iTdXQBjSeEDyWwLQO39URWL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ua..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4ca4be
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6175C7B6 [Sun Oct 24 20:53:10 2021 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	0xc84c4	0xc8600	False	0.891373109014	data	7.83365535264	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xcc000	0x610	0x800	False	0.32958984375	data	3.44849403746	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xce000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/25/21-16:10:51.541596	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58045	8.8.8.8	192.168.2.3
10/25/21-16:10:52.314567	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	2010	192.168.2.3	37.0.10.144
10/25/21-16:10:58.504752	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57875	8.8.8.8	192.168.2.3
10/25/21-16:10:58.580268	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	2010	192.168.2.3	37.0.10.144
10/25/21-16:11:03.350708	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54154	8.8.8.8	192.168.2.3
10/25/21-16:11:03.378268	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	2010	192.168.2.3	37.0.10.144
10/25/21-16:11:08.668535	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	2010	192.168.2.3	37.0.10.144
10/25/21-16:11:14.864387	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	2010	192.168.2.3	37.0.10.144
10/25/21-16:11:20.839143	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64021	8.8.8.8	192.168.2.3
10/25/21-16:11:20.872151	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	2010	192.168.2.3	37.0.10.144
10/25/21-16:11:25.437538	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	2010	192.168.2.3	37.0.10.144
10/25/21-16:11:30.733559	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49749	2010	192.168.2.3	37.0.10.144
10/25/21-16:11:36.896791	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	2010	192.168.2.3	37.0.10.144
10/25/21-16:11:43.084738	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	2010	192.168.2.3	37.0.10.144
10/25/21-16:11:49.752881	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49795	2010	192.168.2.3	37.0.10.144
10/25/21-16:11:56.179155	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49797	2010	192.168.2.3	37.0.10.144
10/25/21-16:12:02.638458	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60352	8.8.8.8	192.168.2.3
10/25/21-16:12:02.676677	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49798	2010	192.168.2.3	37.0.10.144
10/25/21-16:12:06.904246	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56773	8.8.8.8	192.168.2.3
10/25/21-16:12:06.932461	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49799	2010	192.168.2.3	37.0.10.144
10/25/21-16:12:11.265552	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60982	8.8.8.8	192.168.2.3
10/25/21-16:12:11.297453	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49800	2010	192.168.2.3	37.0.10.144
10/25/21-16:12:17.613531	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49815	2010	192.168.2.3	37.0.10.144
10/25/21-16:12:23.599804	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49827	2010	192.168.2.3	37.0.10.144
10/25/21-16:12:29.453867	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50585	8.8.8.8	192.168.2.3
10/25/21-16:12:29.481816	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49828	2010	192.168.2.3	37.0.10.144
10/25/21-16:12:35.390177	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49829	2010	192.168.2.3	37.0.10.144
10/25/21-16:12:39.655133	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49830	2010	192.168.2.3	37.0.10.144

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 25, 2021 16:10:51.521492004 CEST	192.168.2.3	8.8.8.8	0x1039	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 25, 2021 16:10:58.484582901 CEST	192.168.2.3	8.8.8.8	0xa444	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:03.329360962 CEST	192.168.2.3	8.8.8.8	0xb4c	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:08.444194078 CEST	192.168.2.3	8.8.8.8	0x58be	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:14.816983938 CEST	192.168.2.3	8.8.8.8	0x1b05	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:20.819073915 CEST	192.168.2.3	8.8.8.8	0xdb9d	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:25.388521910 CEST	192.168.2.3	8.8.8.8	0x1d2b	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:30.680711031 CEST	192.168.2.3	8.8.8.8	0xda24	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:36.781388044 CEST	192.168.2.3	8.8.8.8	0xa24d	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:43.037879944 CEST	192.168.2.3	8.8.8.8	0xf5c7	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:49.647819042 CEST	192.168.2.3	8.8.8.8	0xca4f	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:56.105796099 CEST	192.168.2.3	8.8.8.8	0x3b3a	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:12:02.618041039 CEST	192.168.2.3	8.8.8.8	0xb25b	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:12:06.804496050 CEST	192.168.2.3	8.8.8.8	0x8118	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:12:11.245232105 CEST	192.168.2.3	8.8.8.8	0xce6c	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:12:17.564661980 CEST	192.168.2.3	8.8.8.8	0xa9ad	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:12:23.551165104 CEST	192.168.2.3	8.8.8.8	0x4f8f	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:12:29.434122086 CEST	192.168.2.3	8.8.8.8	0xa64a	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:12:35.343000889 CEST	192.168.2.3	8.8.8.8	0xdaef	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 25, 2021 16:12:39.608083963 CEST	192.168.2.3	8.8.8.8	0xf833	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)

DNS Answers

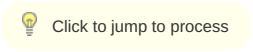
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 16:10:51.541595936 CEST	8.8.8.8	192.168.2.3	0x1039	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:10:58.504751921 CEST	8.8.8.8	192.168.2.3	0xa444	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:03.350708008 CEST	8.8.8.8	192.168.2.3	0xb4c	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:08.460779905 CEST	8.8.8.8	192.168.2.3	0x58be	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:14.835227966 CEST	8.8.8.8	192.168.2.3	0x1b05	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:20.839143038 CEST	8.8.8.8	192.168.2.3	0xdb9d	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:25.409646034 CEST	8.8.8.8	192.168.2.3	0x1d2b	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:30.699050903 CEST	8.8.8.8	192.168.2.3	0xda24	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:36.811371088 CEST	8.8.8.8	192.168.2.3	0xa24d	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:43.056184053 CEST	8.8.8.8	192.168.2.3	0xf5c7	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:11:49.666081905 CEST	8.8.8.8	192.168.2.3	0xca4f	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 16:11:56.124810934 CEST	8.8.8.8	192.168.2.3	0x3b3a	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:12:02.638458014 CEST	8.8.8.8	192.168.2.3	0xb25b	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:12:06.904246092 CEST	8.8.8.8	192.168.2.3	0x8118	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:12:11.265552044 CEST	8.8.8.8	192.168.2.3	0xce6c	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:12:17.582935095 CEST	8.8.8.8	192.168.2.3	0xa9ad	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:12:23.569952965 CEST	8.8.8.8	192.168.2.3	0x4f8f	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:12:29.453866959 CEST	8.8.8.8	192.168.2.3	0xa64a	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:12:35.361471891 CEST	8.8.8.8	192.168.2.3	0xdaef	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)
Oct 25, 2021 16:12:39.626637936 CEST	8.8.8.8	192.168.2.3	0xf833	No error (0)	watermalon 1.sytes.net		37.0.10.144	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: doa8GHSloq.exe PID: 6672 Parent PID: 3572

General

Start time:	16:10:31
Start date:	25/10/2021
Path:	C:\Users\user\Desktop\doa8GHSloq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\doa8GHSloq.exe'
Imagebase:	0x170000
File size:	823808 bytes
MD5 hash:	F85CA66E06121EB29B26D78CC3F64554
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.306901830.0000000002811000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.307288504.0000000003811000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.307288504.0000000003811000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.307288504.0000000003811000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: doa8GHSloq.exe PID: 7164 Parent PID: 6672

General

Start time:	16:10:41
Start date:	25/10/2021
Path:	C:\Users\user\Desktop\doa8GHSloq.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\doa8GHSloq.exe
Imagebase:	0x2a0000
File size:	823808 bytes
MD5 hash:	F85CA66E06121EB29B26D78CC3F64554
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: doa8GHSloq.exe PID: 4820 Parent PID: 6672

General

Start time:	16:10:42
Start date:	25/10/2021
Path:	C:\Users\user\Desktop\doa8GHSloq.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\doa8GHSloq.exe
Imagebase:	0x670000
File size:	823808 bytes
MD5 hash:	F85CA66E06121EB29B26D78CC3F64554
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.360949669.0000000004214000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 3180 Parent PID: 4820

General

Start time:	16:10:45
Start date:	25/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpA5BD.tmp'
Imagebase:	0x11d0000
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: 3912 Parent PID: 3180

General

Start time:	16:10:45
Start date:	25/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: 5700 Parent PID: 4820

General

Start time:	16:10:46
Start date:	25/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true

Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpAC94.tmp'
Imagebase:	0x11d0000
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: doa8GHSloq.exe PID: 3860 Parent PID: 664

General

Start time:	16:10:47
Start date:	25/10/2021
Path:	C:\Users\user\Desktop\doa8GHSloq.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\doa8GHSloq.exe 0
Imagebase:	0xf90000
File size:	823808 bytes
MD5 hash:	F85CA66E06121EB29B26D78CC3F64554
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000E.00000002.326343099.0000000003631000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.327119659.0000000004631000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.327119659.0000000004631000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.327119659.0000000004631000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: conhost.exe PID: 4248 Parent PID: 5700

General

Start time:	16:10:47
Start date:	25/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: dhcpmon.exe PID: 6268 Parent PID: 664

General

Start time:	16:10:50
Start date:	25/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xd50000
File size:	823808 bytes
MD5 hash:	F85CA66E06121EB29B26D78CC3F64554
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: 00000010.00000002.332763752.00000000045F1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.332763752.00000000045F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.332763752.00000000045F1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000010.00000002.331777167.00000000035F1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: doa8GHSloq.exe PID: 5356 Parent PID: 3860

General

Start time:	16:10:52
Start date:	25/10/2021
Path:	C:\Users\user\Desktop\doa8GHSloq.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\doa8GHSloq.exe
Imagebase:	0x500000
File size:	823808 bytes
MD5 hash:	F85CA66E06121EB29B26D78CC3F64554
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: 00000012.00000002.340775979.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.340775979.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.340775979.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.343174730.0000000002CA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.343174730.0000000002CA1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.343333439.0000000003CA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.343333439.0000000003CA1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 6528 Parent PID: 6268

General

Start time:	16:10:53
Start date:	25/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x7b0000
File size:	823808 bytes
MD5 hash:	F85CA66E06121EB29B26D78CC3F64554
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: 00000013.00000002.346641462.00000000031F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.346641462.00000000031F1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.343983482.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.343983482.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.343983482.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.346700520.00000000041F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.346700520.00000000041F1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 6520 Parent PID: 3352

General

Start time:	16:10:53
Start date:	25/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x200000
File size:	823808 bytes
MD5 hash:	F85CA66E06121EB29B26D78CC3F64554
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000014.00000002.337336999.00000000029B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.338194880.00000000039B1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.338194880.00000000039B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.338194880.00000000039B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 4140 Parent PID: 6520

General

Start time:	16:10:56
Start date:	25/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xe00000
File size:	823808 bytes
MD5 hash:	F85CA66E06121EB29B26D78CC3F64554
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.352700590.0000000004641000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.352700590.0000000004641000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.352485340.0000000003641000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.352485340.0000000003641000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.350478158.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.350478158.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.350478158.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis