ID: 357177
Sample Name: 3Fv4j323nj.exe
Cookbook: default.jbs
Time: 09:17:04
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

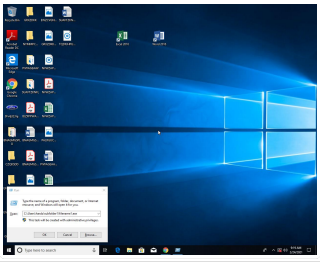
Analysis Report 3Fv4j323nj.exe

Overview

General Information

Sample Name:	3Fv4j323nj.exe
Analysis ID:	357177
MD5:	acfcbd916fa0478..
SHA1:	f2a572347c81b71.
SHA256:	ede5c7b0267f480.
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

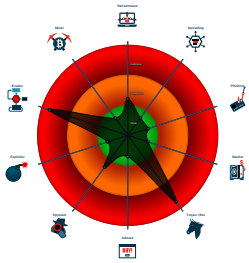
Nanocore GuLoader

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected GuLoader
- Yara detected Nanocore RAT
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Hides that the sample has been dow…
- Hides threads from debuggers
- Tries to detect Any.run

Classification



Startup

- **System is w10x64**
- 3Fv4j323nj.exe (PID: 6520 cmdline: 'C:\Users\user\Desktop\3Fv4j323nj.exe' MD5: ACFCBD916FA04787E4388B339592DD78)
  - RegAsm.exe (PID: 808 cmdline: 'C:\Users\user\Desktop\3Fv4j323nj.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 1748 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 4800 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpE4CC.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 3728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5364 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpE7FA.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5384 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegAsm.exe (PID: 5344 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe 0 MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - conhost.exe (PID: 5412 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 2156 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - conhost.exe (PID: 4000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- filename1.exe (PID: 5044 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: ACFCBD916FA04787E4388B339592DD78)
- dhcpmon.exe (PID: 5736 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - conhost.exe (PID: 1264 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "7c50348d-f4bf-40ba-b0d6-02de82eca13f",
  "Group": "BIZ SALES",
  "Domain1": "194.5.98.182",
  "Domain2": "",
  "Port": 3765,
  "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
0000000C.00000002.503235354.000000002079 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
0000000C.00000002.503235354.000000002079 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
0000000C.00000002.503235354.000000002079 0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000C.00000002.501121759.000000001ED7 7000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000C.00000002.501121759.000000001ED7 7000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x13a3d:$a: NanoCore • 0x13a96:$a: NanoCore • 0x13ad3:$a: NanoCore • 0x13b4c:$a: NanoCore • 0x271f7:$a: NanoCore • 0x2720c:$a: NanoCore • 0x27241:$a: NanoCore • 0x401bb:$a: NanoCore • 0x401d0:$a: NanoCore • 0x40205:$a: NanoCore • 0x13a9f:$b: ClientPlugin • 0x13adc:$b: ClientPlugin • 0x143da:$b: ClientPlugin • 0x143e7:$b: ClientPlugin • 0x26fb3:$b: ClientPlugin • 0x26fce:$b: ClientPlugin • 0x26ffe:$b: ClientPlugin • 0x27215:$b: ClientPlugin • 0x2724a:$b: ClientPlugin • 0x3ff77:$b: ClientPlugin • 0x3ff92:$b: ClientPlugin

Click to see the 6 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.RegAsm.exe.1dd516dc.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
12.2.RegAsm.exe.1dd516dc.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
12.2.RegAsm.exe.1ed8ea94.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0x28771:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost • 0x2879e:$x2: IClientNetworkHost
12.2.RegAsm.exe.1ed8ea94.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x28771:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0x2984c:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost • 0x2878b:$s5: IClientLoggingHost
12.2.RegAsm.exe.1ed8ea94.5.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 21 entries				

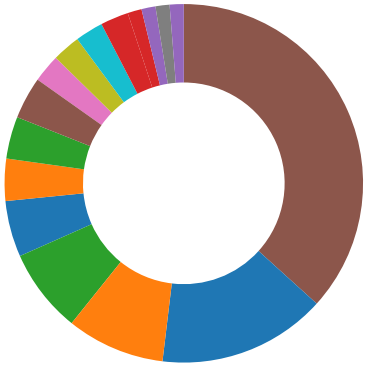
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Binary contains paths to debug symbols

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:

Yara detected GuLoader

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:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

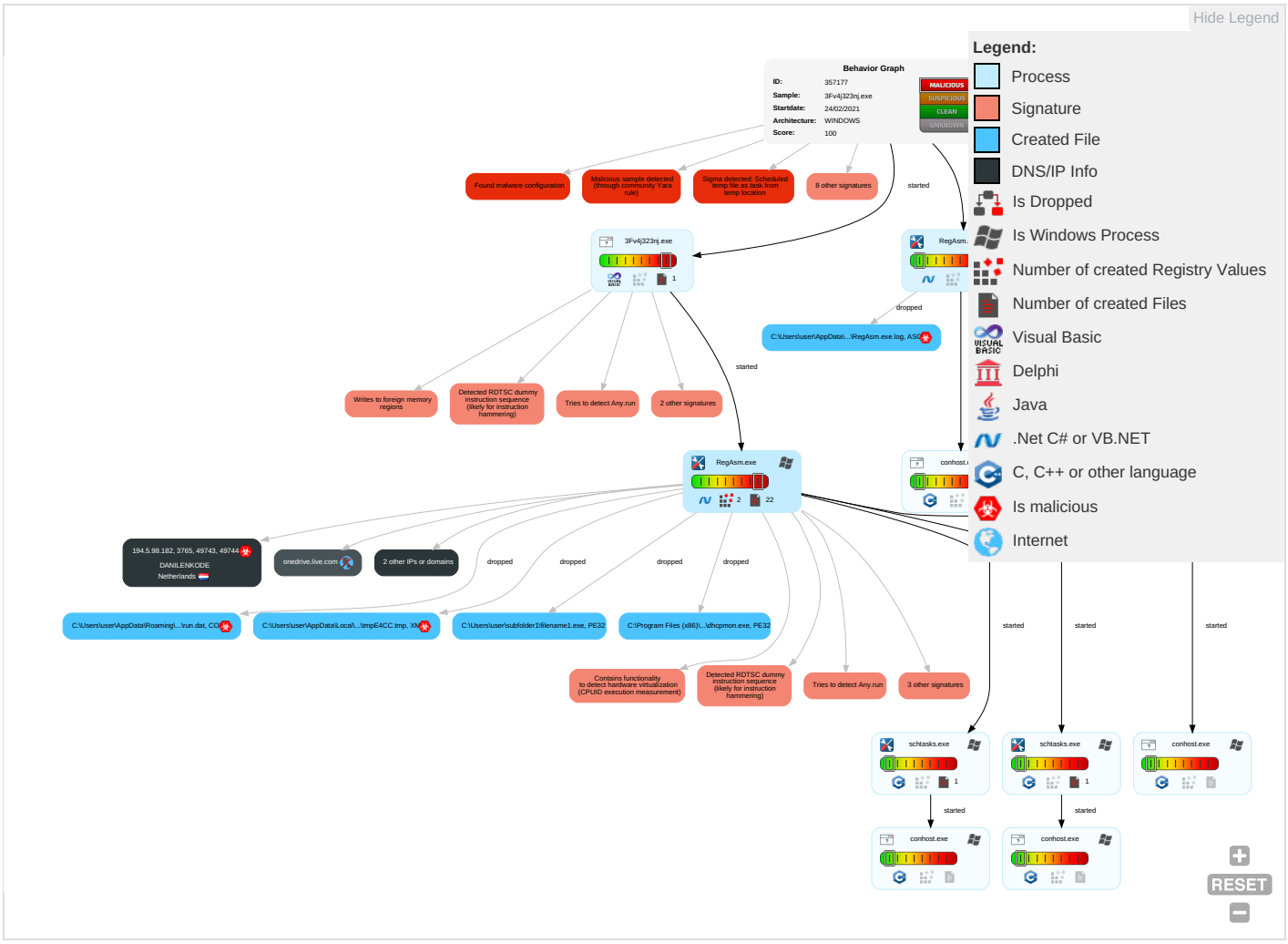
Detected Nanocore Rat

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 1 1	Security Software Discovery 6 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Virtualization/Sandbox Evasion 2 3	LSASS Memory	Virtualization/Sandbox Evasion 2 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	DLL Side-Loading 1	Scheduled Task/Job 1	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	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)	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	DLL Side-Loading 1	Process Injection 1 1 2	LSA Secrets	System Information Discovery 3 1 3	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1	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)	DLL Side-Loading 1	/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

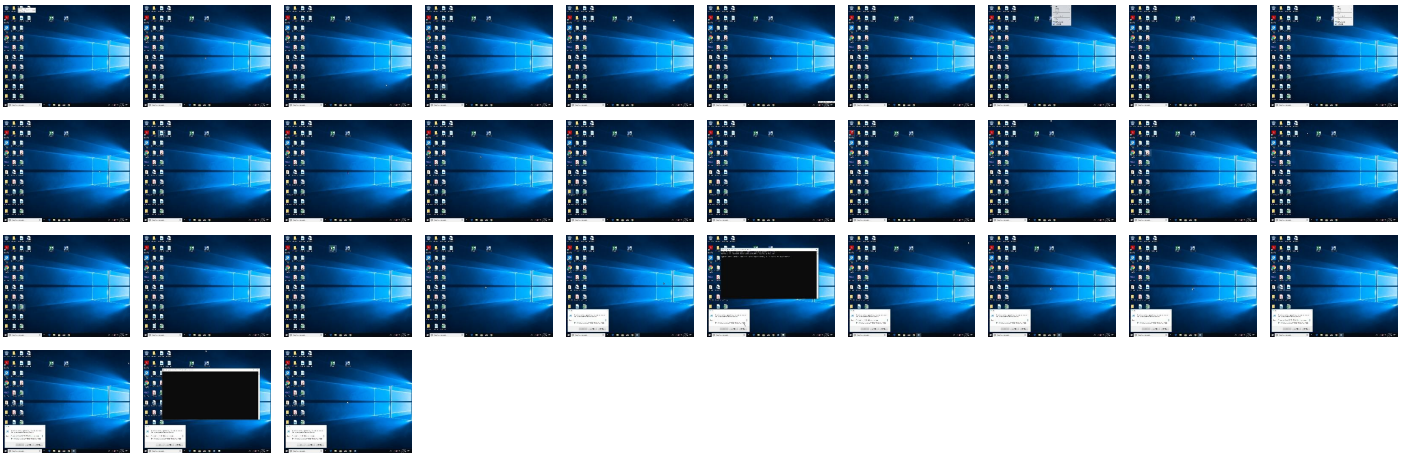
Behavior Graph



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
3Fv4j323nj.exe	13%	Virustotal		Browse
3Fv4j323nj.exe	6%	ReversingLabs	Win32.Infostealer.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\subfolder1\filename1.exe	7%	ReversingLabs	Win32.Infostealer.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.RegAsm.exe.20790000.10.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
194.5.98.182	0%	Virustotal		Browse
194.5.98.182	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
onedrive.live.com	unknown	unknown	false		high
cbavwq.bl.files.1drv.com	unknown	unknown	false		high

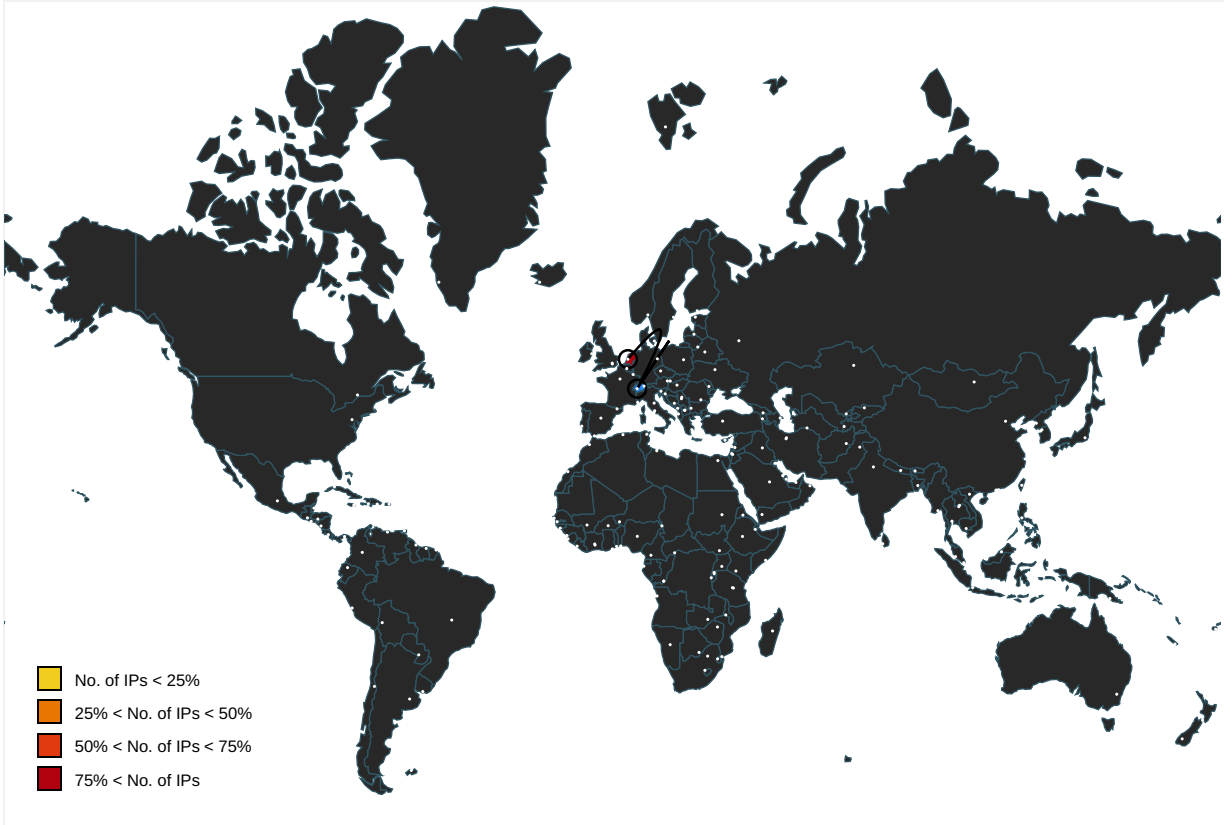
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
194.5.98.182	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/download?cid=F57CEB019EB26E7D&resid=F57CEB019EB26E7D%21106&authkey=AHaSu1X	RegAsm.exe, RegAsm.exe, 00000000C.00000002.482199109.0000000001002000.00000040.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.182	unknown	Netherlands		208476	DANILENKODE	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357177
Start date:	24.02.2021
Start time:	09:17:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3Fv4j323nj.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:	32
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@17/11@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 79.1% (good quality ratio 35.3%) • Quality average: 22.8% • Quality standard deviation: 30.5%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 131.253.33.200, 13.107.22.200, 184.30.21.219, 92.122.145.220, 168.61.161.212, 104.43.139.144, 184.30.20.56, 13.88.21.125, 40.88.32.150, 2.20.142.209, 2.20.142.210, 51.103.5.159, 51.104.139.180, 104.42.151.234, 13.107.42.13, 13.107.42.12, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, au.download.windowsupdate.com.edgesuite.net, odc-web-brs.onedrive.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, storeedgefd.xbetservices.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, l-0004.l-msedge.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, l-0003.l-msedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, odc-bl-files-brs.onedrive.akadns.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, odc-bl-files-geo.onedrive.akadns.net, au-bg-shim.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com, www.bing.com, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, odc-web-geo.onedrive.akadns.net, bl-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, dual-a-0001.dc-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:19:38	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\subfolder1\filename1.exe
09:19:41	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe" s>$(Arg0)
09:19:41	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
09:19:41	API Interceptor	167x Sleep call for process: RegAsm.exe modified
09:19:47	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Time	Type	Description
09:19:55	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\subfolder1\filename1.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.98.182	PO AAN2102002-V020.doc	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	scan09e8902093922023ce.exe	Get hash	malicious	Browse	• 194.5.98.46
	PO AAN2102002-V020.doc	Get hash	malicious	Browse	• 194.5.98.182
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• 194.5.98.202
	neue bestellung.PDF.exe	Get hash	malicious	Browse	• 194.5.97.48
	Orderoffer.exe	Get hash	malicious	Browse	• 194.5.98.66
	neue bestellung.PDF.exe	Get hash	malicious	Browse	• 194.5.97.48
	OrderSuppliesQuote0817916.exe	Get hash	malicious	Browse	• 194.5.97.248
	DHL_6368638172 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 194.5.97.244
	QuotationInvoices.exe	Get hash	malicious	Browse	• 194.5.97.248
	PAYMENT_.EXE	Get hash	malicious	Browse	• 194.5.98.211
	payment.exe	Get hash	malicious	Browse	• 194.5.98.66
	RFQ_1101983736366355 1101938377388.exe	Get hash	malicious	Browse	• 194.5.98.21
	Slip copy .xls.exe	Get hash	malicious	Browse	• 194.5.97.116
	Scan0059.pdf.exe	Get hash	malicious	Browse	• 194.5.97.34
	DHL AWB # 6008824216.png.exe	Get hash	malicious	Browse	• 194.5.97.48
	Scan0019.exe	Get hash	malicious	Browse	• 194.5.97.34
	PurchaseOrdersCSTtyres004786587.exe	Get hash	malicious	Browse	• 194.5.97.248
	Invoice467972.jar	Get hash	malicious	Browse	• 194.5.97.18
	Invoice467972.jar	Get hash	malicious	Browse	• 194.5.97.18
	Hk6Im7DPON.exe	Get hash	malicious	Browse	• 194.5.98.107

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	SecuriteInfo.com.Variant.Razy.845229.13077.exe	Get hash	malicious	Browse	
	document.exe	Get hash	malicious	Browse	
	w0JlVAbpIT.exe	Get hash	malicious	Browse	
	Bjdl7RO0K8.exe	Get hash	malicious	Browse	
	4hW0TZqN01.exe	Get hash	malicious	Browse	
	d4e475d7d17a16be8b9eeac6e10b25af.exe	Get hash	malicious	Browse	
	e5bd3238d220c97cd4d6969abb3b33e0.exe	Get hash	malicious	Browse	
	1c2dec9cbfcd95afe13bf71910fdf95f.exe	Get hash	malicious	Browse	
	Xf6v0G2wIM.exe	Get hash	malicious	Browse	
	jztWD1iKrC.exe	Get hash	malicious	Browse	
	wH22vdkhhU.exe	Get hash	malicious	Browse	
	AqpOn6nwXS.exe	Get hash	malicious	Browse	
	CklrD7MYX2.exe	Get hash	malicious	Browse	
	FahZG6Pdc4.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	61WlCsQR9Q.exe	Get hash	malicious	Browse	
	U7DiqWP9qu.exe	Get hash	malicious	Browse	
	d4x5rl09A7.exe	Get hash	malicious	Browse	
	1WW425NrsA.exe	Get hash	malicious	Browse	
	Kyd6mztyQ5.exe	Get hash	malicious	Browse	
	xdNg7FUNS2.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	53248
Entropy (8bit):	4.490095782293901
Encrypted:	false
SSDEEP:	768:0P2Bbv+VazyoD2z9TU//1mz1+M9GnLEu+2wTFRJS8Ulg:HJv46yoD2BTNz1+M9GLfOw8UO
MD5:	529695608EAFBED00ACA9E61EF333A7C
SHA1:	68CA8B6D8E74FA4F4EE603EB862E36F2A73BC1E5
SHA-256:	44F129DE312409D8A2DF55F655695E1D48D0DB6F20C5C7803EB0032D8E6B53D0
SHA-512:	8FE476E0185B2B0C66F34E51899B932CB35600C753D36FE102BDA5894CDAA58410044E0A30FDBEF76A285C2C75018D7C5A9BA0763D45EC605C2BBD1EBB9ED64
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: SecuriteInfo.com.Variant.Razy.845229.13077.exe, Detection: malicious, Browse • Filename: document.exe, Detection: malicious, Browse • Filename: w0JlVAbpIT.exe, Detection: malicious, Browse • Filename: Bjdl7RO0K8.exe, Detection: malicious, Browse • Filename: 4hW0TZqN01.exe, Detection: malicious, Browse • Filename: d4e475d7d17a16be8b9eeac6e10b25af.exe, Detection: malicious, Browse • Filename: e5bd3238d220c97cd4d6969abb3b33e0.exe, Detection: malicious, Browse • Filename: 1c2dec9cbfcd95afe13bf71910fdf95f.exe, Detection: malicious, Browse • Filename: Xf6v0G2wIM.exe, Detection: malicious, Browse • Filename: jztWD1iKrC.exe, Detection: malicious, Browse • Filename: wH22vdkhhU.exe, Detection: malicious, Browse • Filename: AqpOn6nwXS.exe, Detection: malicious, Browse • Filename: CklrD7MYX2.exe, Detection: malicious, Browse • Filename: FahZG6Pdc4.exe, Detection: malicious, Browse • Filename: 61WlCsQR9Q.exe, Detection: malicious, Browse • Filename: U7DiqWP9qu.exe, Detection: malicious, Browse • Filename: d4x5rl09A7.exe, Detection: malicious, Browse • Filename: 1WW425NrsA.exe, Detection: malicious, Browse • Filename: Kyd6mztyQ5.exe, Detection: malicious, Browse • Filename: xdNg7FUNS2.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z..... ....@.. .....N.... .@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegAsm.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	20
Entropy (8bit):	3.6841837197791887
Encrypted:	false
SSDEEP:	3:QHXMKas:Q3Las
MD5:	B3AC9D09E3A47D5FD00C37E075A70ECB
SHA1:	AD14E6D0E07B00BD10D77A06D68841B20675680B
SHA-256:	7A23C6E7CCD8811ECDF038D3A89D5C7D68ED37324BAE2D4954125D9128FA9432
SHA-512:	09B609EE1061205AA45B3C954EFC6C1A03C8FD6B3011FF88CF2C060E19B1D7FD51EE0CB9D02A39310125F3A66AA0146261BDEE3D804F472034DF711BC942E31
Malicious:	**true**
Preview:	1,"fusion","GAC",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:	modified
Size (bytes):	20
Entropy (8bit):	3.6841837197791887
Encrypted:	false
SSDEEP:	3:QHXMKas:Q3Las
MD5:	B3AC9D09E3A47D5FD00C37E075A70ECB
SHA1:	AD14E6D0E07B00BD10D77A06D68841B20675680B
SHA-256:	7A23C6E7CCD8811ECDF038D3A89D5C7D68ED37324BAE2D4954125D9128FA9432
SHA-512:	09B609EE1061205AA45B3C954EFC6C1A03C8FD6B3011FF88CF2C060E19B1D7FD51EE0CB9D02A39310125F3A66AA0146261BDEE3D804F472034DF711BC942E31
Malicious:	false
Preview:	1,"fusion","GAC",0..

C:\Users\user\AppData\Local\Temp\tmpE4CC.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1319
Entropy (8bit):	5.133606110275315
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mne5xtn:cbk4oL600QydbQxIYODOLedq3Ze5j
MD5:	C6F0625BF4C1CDFB699980C9243D3B22
SHA1:	43DE1FE5805769355163 27F17B5DA0C656C72851
SHA-256:	8DFC4E937F0B2374E3CED25FCE344B0731CF44B8854625B318D50ECE2DA8F576
SHA-512:	9EF2DBD4142AD0E1E6006929376ECB8011E7FFC801EE2101E906787D70325AD82752DF65839DE9972391FA52E1E5974EC1A5C7465A88AA56257633EBB7D70969
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\tmpE7FA.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.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\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	COM executable for DOS
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:EF:EF
MD5:	6E49A312690E315F4BC2BA43AF4030EC

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SHA1:	9A9D72CD8DEE34F0255903E39783F6B8FAB4D319
SHA-256:	5F595A3E8DD84AE806A7D2D31169D6C698FFB74CE24CCC14B2549030E1D6BAC3
SHA-512:	AD53023FF9C31AF49E313DCE09A7E7338EAAE29DFF44A7B963F82FAA7DC679393DE3AD1C079C343EED743E33DB3B7BD00F98004542336F8C02F71554DDD6A25
Malicious:	**true**
Preview:	...^...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	56
Entropy (8bit):	4.787365359936823
Encrypted:	false
SSDEEP:	3:oMty8WbSXgL4A:oMLWuQL4A
MD5:	EFD1636CFC3CC38FD7BABAE5CAC9EDE0
SHA1:	4D7D378ABEB682EEFBD039930C0EA996FBF54178
SHA-256:	F827D5B11C1EB3902D601C3E0B59BA32FE11C0B573FBF22FB2AF86BFD4651BBA
SHA-512:	69B2B0AB1A6E13395EF52DCB903B8E17D842E6D0D44F801FF2659CFD5EC343C8CC57928B02961FC7099AD43FF05633BAF5AC39042A00C8676D4FA8F6F8C2A5D7
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

C:\Users\user\subfolder1\filename1.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	4.85840802848053
Encrypted:	false
SSDEEP:	3072:FwVUPYLV4+aQTxxs+7Qx+2OGeoyrARHNlyCI2jnyIa3MAB+f/FwGIt1KFzOn1k4H:FwVUPYLV4+aQTxxs+7Qx+2OGeoyrARHs
MD5:	ACFCBD916FA04787E4388B339592DD78
SHA1:	F2A572347C81B71C3A59F00A37F68DB698715460
SHA-256:	EDE5C7B0267F4801A7BEBB22A18035923E71A476CEB3B9D94F582AA199DEB3F0
SHA-512:	23B895AD239AC48726A1446299E4534E496BB891530CB11E3764FB871F5F5097B12CCE346FDBCFE4A1C31D46F31A25CE407B17D6AB1A141BEEF9613E92DA817
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 7%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~..0.....0...Rich1.....PE..L....$T.....P. .....`....@.....TY..(....p.....(... .....text....M.....P..... ..`.data.....`.....`.....@....rsrc.....p.....p.....@..@...I.....MSVBVM60.DLL..... ....

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1010
Entropy (8bit):	4.298581893109255
Encrypted:	false
SSDEEP:	24:zKTDwL/0XZd3Wo3opQ5ZKBQFYVgt7ovrNOYlK:zKTDwAXZxo4ABV+SrUYE
MD5:	367EEEC425FE7E80B723298C447E2F22
SHA1:	3873DFC88AF504FF79231FE2BF0E3CD93CE45195
SHA-256:	481A7A3CA0DD32DA4772718BA4C1EF3F01E8D184FE82CF6E9C5386FD343264BC
SHA-512:	F7101541D87F045E9DBC45941CDC5A7F97F3EFC29AC0AF2710FC24FA64F0163F9463DE373A5D2BE1270126829DE81006FB8E764186374966E8D0E9BB35B7D7D6
Malicious:	false
Preview:	Microsoft (R) .NET Framework Assembly Registration Utility 2.0.50727.8922..Copyright (C) Microsoft Corporation 1998-2004. All rights reserved.....Syntax: RegAsm AssemblyName [Options]..Options:.. /unregister Unregister types.. /tlb[:FileName] Export the assembly to the specified type library.. and register it.. /regfile[:FileName] Generate a reg file with the specified name.. instead of registering the types. This option.. cannot be used with the /u or /tlb options.. /codebase Set the code base in the registry.. /registered Only refer to already registered type libraries.. /asmpath:Directory Look for assembly references here.. /nologo Prevents RegAsm from displaying logo.. /silent Silent mode. Prevents displaying of success messages.. /verbose Displays extra information.. /? or /help Display this usage

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.85840802848053
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	3Fv4j323nj.exe
File size:	131072
MD5:	acfcbd916fa04787e4388b339592dd78
SHA1:	f2a572347c81b71c3a59f00a37f68db698715460
SHA256:	ede5c7b0267f4801a7bebb22a18035923e71a476ceb3b9d94f582aa199deb3f0
SHA512:	23b895ad239ac48726a1446299e4534e496bb891530cb11e3764fb871f5f5097b12cce346fdbcfe4a1c31d46f31a25ce407b17d6ab1a141beef9613e92da817e
SSDEEP:	3072:FwVUPYLV4+aQTxxs+7Qx+2OGeoyrARHNlyCI2jnyla3MAB+f/FwGIt1KFzOn1k4H:FwVUPYLV4+aQTxxs+7Qx+2OGeoyrARHs
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L.....$T.....P.....`....@.....

File Icon

Icon Hash:	01d292796dda0080

Static PE Info

General

Entrypoint:	0x4013dc
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5424AED4 [Fri Sep 26 00:09:56 2014 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	cc882d101998a701353b40b0cd8c341a

Entrypoint Preview

Instruction
push 00412774h
call 00007F4684C461D3h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al

Instruction
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax-61h], dl
sub dword ptr [edx+ebx*8], ebx
or al, 66h
dec esi
mov eax, 1FB77221h
sbb cl, byte ptr [ecx+2Eh]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
dec ebp
inc ecx
inc edi
dec ecx
push ebx
push esp
inc ebp
push edx
add byte ptr [eax], al
add byte ptr [eax], al
jecxz 00007F4684C461EFh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
add al, C9h
pop ecx
and ch, cl
hlt
pushad
out 43h, al
mov ch, 90h
fdiv qword ptr [edi-37F9A4A3h]
inc ebx
imul ebx, dword ptr [ebx+eax*4+04h], B74A52B6h
adc dh, byte ptr [ebx-52h]
mov dh, A6h
mov byte ptr [eax+33AD4F3Ah], FFFFFF99h
iretw
adc dword ptr [edi+00AA000Ch], esi
pushad
rcl dword ptr [ebx+00000000h], cl
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xchg eax, ebp
adc al, byte ptr [ecx]
add byte ptr [esi+0000007Fh], dl
pop es
add byte ptr [ecx+67h], cl
outsb
aaa
add byte ptr [66000801h], cl
insb
insb
popad
bound ebp, dword ptr [ebp+00h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x15954	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x17000	0x83d6	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0xe0	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x14d84	0x15000	False	0.395542689732	data	5.53569539518	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x16000	0xa18	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x83d6	0x9000	False	0.340196397569	data	3.52970620397	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1f2ae	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1dc86	0x1628	dBase IV DBT of \200.DBF, blocks size 0, block length 4608, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x1bfde	0x1ca8	data		
RT_ICON	0x1b336	0xca8	data		
RT_ICON	0x1afce	0x368	GLS_BINARY_LSB_FIRST		
RT_ICON	0x18a26	0x25a8	data		
RT_ICON	0x1797e	0x10a8	data		
RT_ICON	0x17516	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x174a0	0x76	data		
RT_VERSION	0x17240	0x260	data		

Imports

DLL	Import

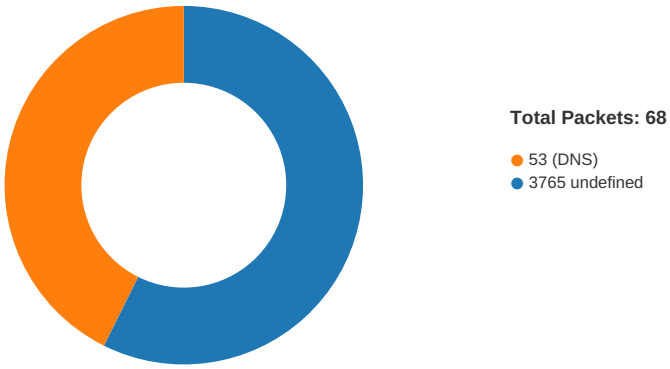
DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaLateMemCall, __vbaVarDup, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0000 0x04b0
InternalName	trenchlet
FileVersion	1.00
CompanyName	Sinth Radio
ProductName	Sinth Radio
ProductVersion	1.00
FileDescription	Sinth Radio
OriginalFilename	trenchlet.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 09:19:41.300220966 CET	49743	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:19:41.379900932 CET	3765	49743	194.5.98.182	192.168.2.3
Feb 24, 2021 09:19:41.881926060 CET	49743	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:19:41.961496115 CET	3765	49743	194.5.98.182	192.168.2.3
Feb 24, 2021 09:19:42.475744963 CET	49743	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:19:42.558160067 CET	3765	49743	194.5.98.182	192.168.2.3
Feb 24, 2021 09:19:46.663628101 CET	49744	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:19:46.731425047 CET	3765	49744	194.5.98.182	192.168.2.3
Feb 24, 2021 09:19:47.241864920 CET	49744	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:19:47.310600996 CET	3765	49744	194.5.98.182	192.168.2.3
Feb 24, 2021 09:19:47.851201057 CET	49744	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:19:47.918890953 CET	3765	49744	194.5.98.182	192.168.2.3
Feb 24, 2021 09:19:51.932102919 CET	49745	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:19:51.999983072 CET	3765	49745	194.5.98.182	192.168.2.3
Feb 24, 2021 09:19:52.554655075 CET	49745	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:19:52.624054909 CET	3765	49745	194.5.98.182	192.168.2.3
Feb 24, 2021 09:19:53.242300034 CET	49745	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:19:53.311188936 CET	3765	49745	194.5.98.182	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 09:19:57.352601051 CET	49746	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:19:57.420849085 CET	3765	49746	194.5.98.182	192.168.2.3
Feb 24, 2021 09:19:58.055802107 CET	49746	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:19:58.123481989 CET	3765	49746	194.5.98.182	192.168.2.3
Feb 24, 2021 09:19:58.742737055 CET	49746	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:19:58.810707092 CET	3765	49746	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:02.888335943 CET	49750	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:02.957760096 CET	3765	49750	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:03.556118011 CET	49750	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:03.623994112 CET	3765	49750	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:04.244697094 CET	49750	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:04.312689066 CET	3765	49750	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:08.332813025 CET	49751	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:08.412843943 CET	3765	49751	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:09.056123972 CET	49751	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:09.135972977 CET	3765	49751	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:09.743658066 CET	49751	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:09.825552940 CET	3765	49751	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:13.889895916 CET	49752	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:13.957961082 CET	3765	49752	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:14.556612968 CET	49752	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:14.624669075 CET	3765	49752	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:15.244081974 CET	49752	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:15.312050104 CET	3765	49752	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:19.327959061 CET	49753	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:19.397562027 CET	3765	49753	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:20.057024956 CET	49753	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:20.127264977 CET	3765	49753	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:20.744601965 CET	49753	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:20.812661886 CET	3765	49753	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:24.866000891 CET	49754	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:24.945856094 CET	3765	49754	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:25.557502031 CET	49754	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:25.637367010 CET	3765	49754	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:26.151344061 CET	49754	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:26.231223106 CET	3765	49754	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:30.285603046 CET	49755	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:30.353274107 CET	3765	49755	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:30.854815960 CET	49755	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:30.923059940 CET	3765	49755	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:31.558011055 CET	49755	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:31.626044989 CET	3765	49755	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:35.653356075 CET	49756	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:35.721105099 CET	3765	49756	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:36.245901108 CET	49756	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:36.315162897 CET	3765	49756	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:36.855320930 CET	49756	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:36.923559904 CET	3765	49756	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:40.971987009 CET	49757	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:41.051913023 CET	3765	49757	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:41.558893919 CET	49757	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:41.639123917 CET	3765	49757	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:42.246387005 CET	49757	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:42.326005936 CET	3765	49757	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:46.366910934 CET	49758	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:46.446589947 CET	3765	49758	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:47.052978039 CET	49758	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:47.133605003 CET	3765	49758	194.5.98.182	192.168.2.3
Feb 24, 2021 09:20:47.746603966 CET	49758	3765	192.168.2.3	194.5.98.182
Feb 24, 2021 09:20:47.827811956 CET	3765	49758	194.5.98.182	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 09:17:48.956769943 CET	51281	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:17:48.980241060 CET	49199	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:17:49.011619091 CET	53	51281	8.8.8.8	192.168.2.3
Feb 24, 2021 09:17:49.034463882 CET	53	49199	8.8.8.8	192.168.2.3
Feb 24, 2021 09:17:49.705398083 CET	50620	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:17:49.766128063 CET	53	50620	8.8.8.8	192.168.2.3
Feb 24, 2021 09:17:50.123684883 CET	64938	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:17:50.175513029 CET	53	64938	8.8.8.8	192.168.2.3
Feb 24, 2021 09:17:51.459873915 CET	60152	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:17:51.511327028 CET	53	60152	8.8.8.8	192.168.2.3
Feb 24, 2021 09:17:51.698739052 CET	57544	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:17:51.757580042 CET	53	57544	8.8.8.8	192.168.2.3
Feb 24, 2021 09:17:52.751905918 CET	55984	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:17:52.803951979 CET	53	55984	8.8.8.8	192.168.2.3
Feb 24, 2021 09:17:54.673037052 CET	64185	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:17:54.724788904 CET	53	64185	8.8.8.8	192.168.2.3
Feb 24, 2021 09:17:56.019535065 CET	65110	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:17:56.073129892 CET	53	65110	8.8.8.8	192.168.2.3
Feb 24, 2021 09:17:57.311530113 CET	58361	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:17:57.360574961 CET	53	58361	8.8.8.8	192.168.2.3
Feb 24, 2021 09:17:59.473475933 CET	63492	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:17:59.523004055 CET	53	63492	8.8.8.8	192.168.2.3
Feb 24, 2021 09:18:00.629548073 CET	60831	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:18:00.681612015 CET	53	60831	8.8.8.8	192.168.2.3
Feb 24, 2021 09:18:22.192106009 CET	60100	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:18:22.251553059 CET	53	60100	8.8.8.8	192.168.2.3
Feb 24, 2021 09:18:36.506161928 CET	53195	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:18:36.555207014 CET	53	53195	8.8.8.8	192.168.2.3
Feb 24, 2021 09:18:37.859616995 CET	50141	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:18:37.908946037 CET	53	50141	8.8.8.8	192.168.2.3
Feb 24, 2021 09:18:38.950968981 CET	53023	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:18:39.000190973 CET	53	53023	8.8.8.8	192.168.2.3
Feb 24, 2021 09:18:40.336797953 CET	49563	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:18:40.388636112 CET	53	49563	8.8.8.8	192.168.2.3
Feb 24, 2021 09:18:42.263293982 CET	51352	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:18:42.326663017 CET	53	51352	8.8.8.8	192.168.2.3
Feb 24, 2021 09:18:43.296252966 CET	59349	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:18:43.347326040 CET	53	59349	8.8.8.8	192.168.2.3
Feb 24, 2021 09:19:03.862909079 CET	57084	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:19:03.911844015 CET	53	57084	8.8.8.8	192.168.2.3
Feb 24, 2021 09:19:07.624607086 CET	58823	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:19:07.687391043 CET	53	58823	8.8.8.8	192.168.2.3
Feb 24, 2021 09:19:13.906763077 CET	57568	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:19:13.955673933 CET	53	57568	8.8.8.8	192.168.2.3
Feb 24, 2021 09:19:15.050631046 CET	50540	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:19:15.109963894 CET	53	50540	8.8.8.8	192.168.2.3
Feb 24, 2021 09:19:16.576379061 CET	54366	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:19:16.625118971 CET	53	54366	8.8.8.8	192.168.2.3
Feb 24, 2021 09:19:17.980823040 CET	53034	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:19:18.052654028 CET	53	53034	8.8.8.8	192.168.2.3
Feb 24, 2021 09:19:36.900980949 CET	57762	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:19:36.952677965 CET	53	57762	8.8.8.8	192.168.2.3
Feb 24, 2021 09:19:37.573504925 CET	55435	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:19:37.661463976 CET	53	55435	8.8.8.8	192.168.2.3
Feb 24, 2021 09:19:39.585629940 CET	50713	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:19:39.637490988 CET	53	50713	8.8.8.8	192.168.2.3
Feb 24, 2021 09:19:57.256592989 CET	56132	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:19:57.318309069 CET	53	56132	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 09:19:36.900980949 CET	192.168.2.3	8.8.8.8	0xa4b6	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 09:19:37.573504925 CET	192.168.2.3	8.8.8.8	0xbee7	Standard query (0)	cbavwq.bl.files.1drv.com	A (IP address)	IN (0x0001)

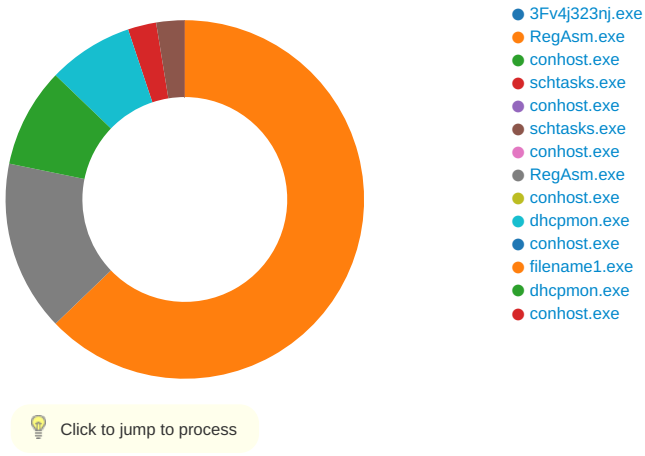
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2021 09:19:36.952677965 CET	8.8.8.8	192.168.2.3	0xa4b6	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 09:19:37.661463976 CET	8.8.8.8	192.168.2.3	0xbee7	No error (0)	cbavwq.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 09:19:37.661463976 CET	8.8.8.8	192.168.2.3	0xbee7	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 3Fv4j323nj.exe PID: 6520 Parent PID: 5724

General

Start time:	09:17:58
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\3Fv4j323nj.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\3Fv4j323nj.exe'
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	ACFCBD916FA04787E4388B339592DD78
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 808 Parent PID: 6520

General

Start time:	09:19:21
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\3Fv4j323nj.exe'
Imagebase:	0xc30000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.503235354.0000000020790000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.503235354.0000000020790000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.503235354.0000000020790000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.501121759.000000001ED77000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.501121759.000000001ED77000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 0000000C.00000002.482199109.0000000001002000.00000040.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.502878730.0000000020500000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.502878730.0000000020500000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\subfolder1\filename1.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1007766	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1004519	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1004519	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1004519	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1004519	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1004519	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1004519	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	200A07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	200A089B	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	200A07A1	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	200A0B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpE4CC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	200A0D1C	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	200A089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpE7FA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	200A0D1C	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	200A07A1	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	200A07A1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE4CC.tmp	success or wait	1	1DB9BF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE7FA.tmp	success or wait	1	1DB9BF0E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\subfolder1\filename1.exe	unknown	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 75 9f f9 db 31 fe 97 88 31 fe 97 88 31 fe 97 88 b2 e2 99 88 30 fe 97 88 7e dc 9e 88 30 fe 97 88 07 d8 9a 88 30 fe 97 88 52 69 63 68 31 fe 97 88 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 d4 ae 24 54 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 50 01 00 00 a0 00 00 00 00 00 00 dc 13 00 00 00 10 00 00 00 60 01 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......u...1...1...1.......0. ..~...0.......0...Rich1....... ....PE..L.....$T............. ...P...................`....@.	success or wait	1	1001C6F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	b8 d7 0e 5e e8 d8 d8 48	...^...H	success or wait	1	200A0A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	53248	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 d4 cc 7b 5a 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 a0 00 00 00 20 00 00 00 00 00 00 de b7 00 00 00 20 00 00 00 c0 00 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 01 00 00 10 00 00 4e c1 01 00 03 00 40 05 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......PE..L..... {Z.................... ....@.. ....N.....@................	success or wait	1	200A0B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpE4CC.tmp	unknown	1319	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	200A0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	56	43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 32 2e 30 2e 35 30 37 32 37 5c 52 65 67 41 73 6d 2e 65 78 65	C:\Windows\Microsoft.NET \Framework\v2.0.50727\RegAsm.exe	success or wait	1	200A0A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE7FA.tmp	unknown	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	200A0A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\3Fv4j323nj.exe	unknown	131072	success or wait	1	1007766	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	200A0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	success or wait	1	200A0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	end of file	1	200A0A53	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	Startup key	unicode	C:\Users\user\subfolder1\filename1.exe	success or wait	1	10017E4	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	200A0C12	RegSetValueExW

Analysis Process: conhost.exe PID: 1748 Parent PID: 808

General

Start time:	09:19:22
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 4800 Parent PID: 808

General

Start time:	09:19:39
Start date:	24/02/2021
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\tmpE4CC.tmp'
Imagebase:	0x1b0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE4CC.tmp	unknown	2	success or wait	1	1BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE4CC.tmp	unknown	1320	success or wait	1	1BABD9	ReadFile

Analysis Process: conhost.exe PID: 3728 Parent PID: 4800

General

Start time:	09:19:40
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 5364 Parent PID: 808

General

Start time:	09:19:40
Start date:	24/02/2021
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\tmpE7FA.tmp'
Imagebase:	0x1b0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE7FA.tmp	unknown	2	success or wait	1	1BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE7FA.tmp	unknown	1311	success or wait	1	1BABD9	ReadFile

Analysis Process: conhost.exe PID: 5384 Parent PID: 5364

General

Start time:	09:19:40
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 5344 Parent PID: 528

General

Start time:	09:19:41
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe 0
Imagebase:	0x80000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegAsm.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	7266DCB3	unknown
\Device\ConDrv	unknown	147	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 41 73 73 65 6d 62 6c 79 20 52 65 67 69 73 74 72 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 20 31 39 39 38 2d 32 30 30 34 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Assembly Registration Utility 2 .0.50727.8922..Copyright (C) Microsoft Corporation 1998-2004. All rights reserved.....	success or wait	1	7266DFAB	unknown
\Device\ConDrv	unknown	0			success or wait	1	7266DCB3	unknown
\Device\ConDrv	unknown	89	52 65 67 41 73 6d 20 3a 20 65 72 72 6f 72 20 52 41 30 30 30 30 20 3a 20 55 6e 61 62 6c 65 20 74 6f 20 6c 6f 63 61 74 65 20 69 6e 70 75 74 20 61 73 73 65 6d 62 6c 79 20 27 30 27 20 6f 72 20 6f 6e 65 20 6f 66 20 69 74 73 20 64 65 70 65 6e 64 65 6e 63 69 65 73 2e 0d 0a	RegAsm : error RA0000 : Unable to locate input assembly '0' or one of its dependencies...	success or wait	1	7266DFAB	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegAsm.exe.log	unknown	20	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a	1,"fusion","GAC",0..	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FE5544	unknown

Analysis Process: conhost.exe PID: 5412 Parent PID: 5344

General

Start time:	09:19:41
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 2156 Parent PID: 528

General

Start time:	09:19:41
Start date:	24/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x6c0000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	20	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a	1,"fusion","GAC",0..	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown

Analysis Process: conhost.exe PID: 4000 Parent PID: 2156

General

Start time:	09:19:41
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: filename1.exe PID: 5044 Parent PID: 3388

General

Start time:	09:19:47
Start date:	24/02/2021
Path:	C:\Users\user\subfolder1\filename1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\subfolder1\filename1.exe'
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	ACFCBD916FA04787E4388B339592DD78
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 7%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: dhcpmon.exe PID: 5736 Parent PID: 3388

General

Start time:	09:19:55
Start date:	24/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x10000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	209A53F	WriteFile
\Device\ConDrv	unknown	147	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 41 73 73 65 6d 62 6c 79 20 52 65 67 69 73 74 72 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 20 31 39 39 38 2d 32 30 30 34 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Assembly Registration Utility 2 .0.50727.8922..Copyright (C) Microsoft Corporation 1998-2004. All rights reserved.....	success or wait	1	209A53F	WriteFile
\Device\ConDrv	unknown	49	53 79 6e 74 61 78 3a 20 52 65 67 41 73 6d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 20 5b 4f 70 74 69 6f 6e 73 5d 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a	Syntax: RegAsm AssemblyName [O ptions]..Options:..	success or wait	14	209A53F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown

Analysis Process: conhost.exe PID: 1264 Parent PID: 5736

General

Start time:	09:19:55
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis