ID: 357184
Sample Name: V33QokMrIv.exe
Cookbook: default.jbs
Time: 09:23:21
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

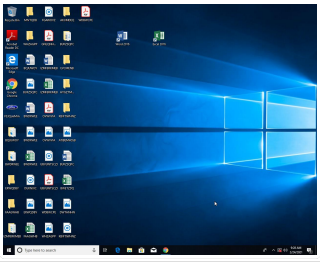
Analysis Report V33QokMrIv.exe

Overview

General Information

Sample Name:	V33QokMrIv.exe
Analysis ID:	357184
MD5:	e18dbe57194dd7..
SHA1:	76bacc8c5fbbf67..
SHA256:	b5d510179ab07f0.
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

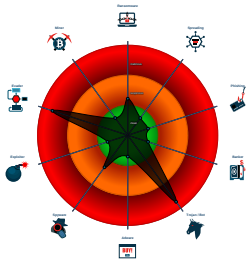
Nanocore GuLoader

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected GuLoader
- Yara detected Nanocore RAT
- C2 URLs / IPs found in malware con…
- Detected RDTSC dummy instruction…
- Hides that the sample has been dow…
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- V33QokMrIv.exe (PID: 6352 cmdline: 'C:\Users\user\Desktop\V33QokMrIv.exe' MD5: E18DBE57194DD717D54A907BA8E6D3E1)
  - taskhostw.exe (PID: 6556 cmdline: taskhostw.exe None MD5: CE95E236FC9FE2D6F16C926C75B18BAF)
    - conhost.exe (PID: 5664 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5496 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp7CFF.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5516 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp801C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6520 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegAsm.exe (PID: 6556 cmdline: 'C:\Users\user\Desktop\V33QokMrIv.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
- RegAsm.exe (PID: 768 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe 0 MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - conhost.exe (PID: 6012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 2936 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - conhost.exe (PID: 4244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- filename1.exe (PID: 6092 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: E18DBE57194DD717D54A907BA8E6D3E1)
- dhcpmon.exe (PID: 6896 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - conhost.exe (PID: 6864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- filename1.exe (PID: 6980 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: E18DBE57194DD717D54A907BA8E6D3E1)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "92421eeb-c456-44c2-ab8d-5a66d7e5ab97",
  "Group": "Company",
  "Domain1": "194.5.98.202",
  "Domain2": "",
  "Port": 4488,
  "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
0000000F.00000002.1253583807.000000001EDB3000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000F.00000002.1187103126.0000000001002000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 6556	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Process Memory Space: RegAsm.exe PID: 6556	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 6556	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x92f9:$a: NanoCore • 0x9326:$a: NanoCore • 0x937f:$a: NanoCore • 0x10b8e:$a: NanoCore • 0x10ba1:$a: NanoCore • 0x10bd3:$a: NanoCore • 0x1a664:$a: NanoCore • 0x1a691:$a: NanoCore • 0x1a6ea:$a: NanoCore • 0x21ef9:$a: NanoCore • 0x21f0c:$a: NanoCore • 0x21f3e:$a: NanoCore • 0x959c8:$a: NanoCore • 0x95bf2:$a: NanoCore • 0xcbe10:$a: NanoCore • 0x147046:$a: NanoCore • 0x147270:$a: NanoCore • 0x17720b:$a: NanoCore • 0x1772ac:$a: NanoCore • 0x177319:$a: NanoCore • 0x1773da:$a: NanoCore

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
15.2.RegAsm.exe.1dd712f8.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
15.2.RegAsm.exe.1dd712f8.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
15.2.RegAsm.exe.1edc7a58.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
15.2.RegAsm.exe.1edc7a58.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
15.2.RegAsm.exe.1edc7a58.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 6 entries				

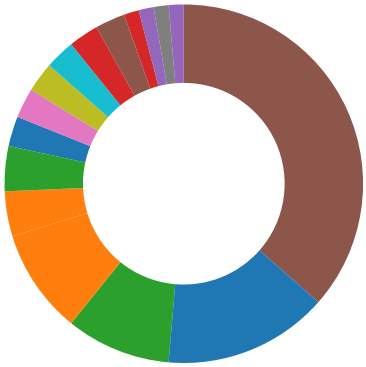
Sigma Overview

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

Yara detected Nanocore RAT

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Binary contains paths to debug symbols

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:

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:

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

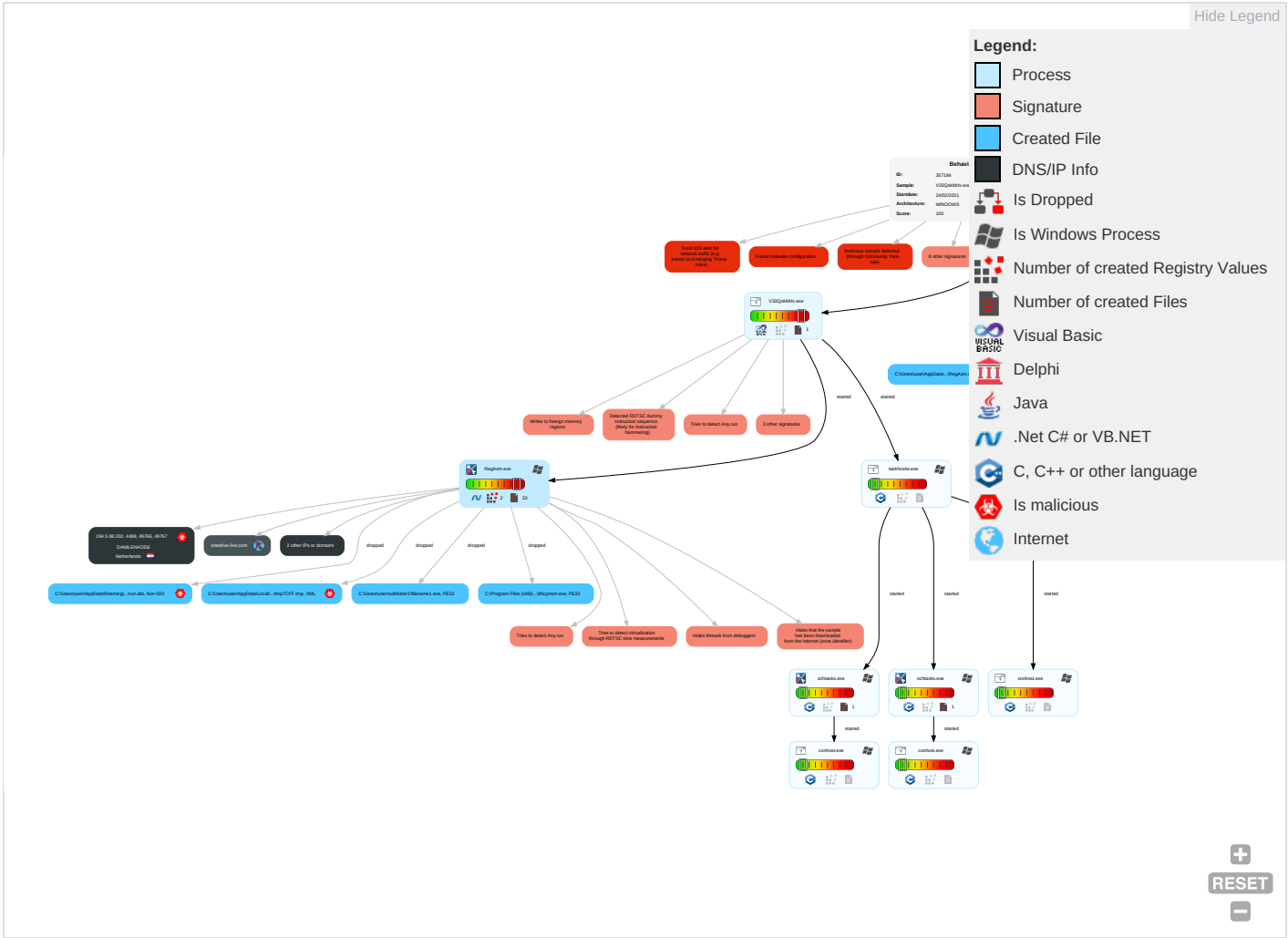
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 2	Input Capture 1 1	Security Software Discovery 5 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networl Commu

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	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	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	DLL Side-Loading 1	Registry Run Keys / Startup Folder 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	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	DLL Side-Loading 1	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Information Discovery 2 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

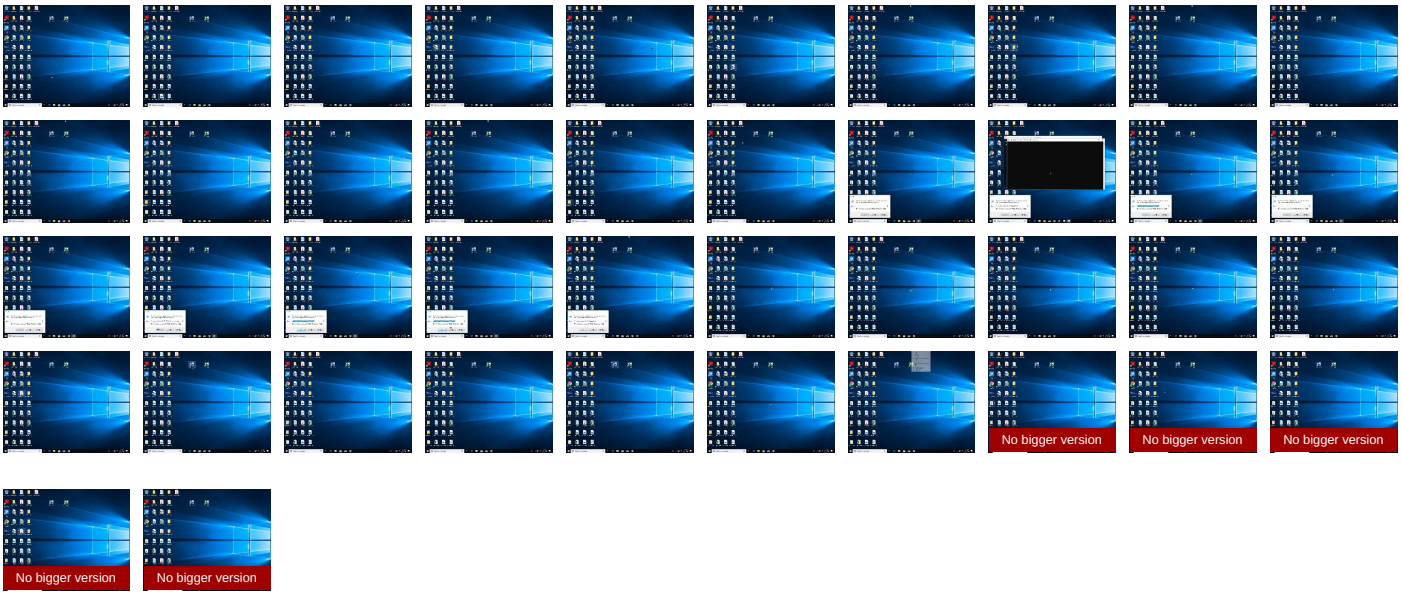
Behavior Graph



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
V33QokMrIv.exe	9%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
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	9%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
194.5.98.202	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

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

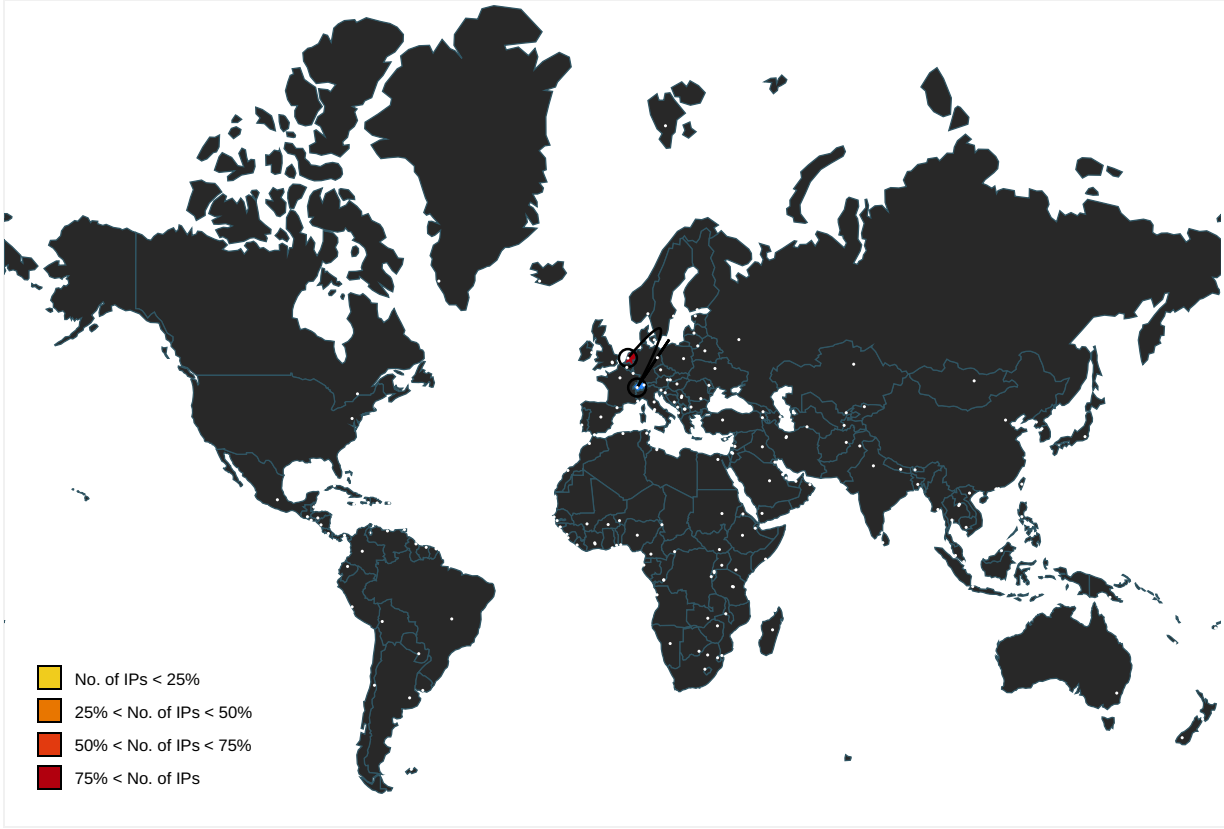
Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ibkebw.dm.files.1drv.com/	RegAsm.exe, 0000000F.00000002.1191880037.00000000014AB000.00000004.00000020.sdmp	false		high
http://https://onedrive.live.com/download?cid=802AC8A73EEC8C8E&resid=802AC8A73EEC8C8E%21110&authkey=AK1w6-P	RegAsm.exe, RegAsm.exe, 0000000F.00000002.1191880037.00000000014AB000.00000004.00000020.sdmp	false		high
http://https://onedrive.live.com/zZm	RegAsm.exe, 0000000F.00000002.1191880037.00000000014AB000.00000004.00000020.sdmp	false		high
http://https://ibkebw.dm.files.1drv.com/y4m_7vjlVAP2dktIZ7ToWB_X8Tx5mpxc0CHqB4Dc4Xc8QJNrWia8ZAB0h8vRJGCEryL	RegAsm.exe, 0000000F.00000003.1173973223.000000000150D000.00000004.00000001.sdmp, RegAsm.exe, 0000000F.00000002.1191919663.00000000014FB000.00000004.00000020.sdmp	false		high
http://https://onedrive.live.com/	RegAsm.exe, 0000000F.00000002.1191880037.00000000014AB000.00000004.00000020.sdmp	false		high
http://https://ibkebw.dm.files.1drv.com/Jep	RegAsm.exe, 0000000F.00000002.1191880037.00000000014AB000.00000004.00000020.sdmp	false		high

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357184
Start date:	24.02.2021
Start time:	09:23:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	V33QokMrIv.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:	30
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@19/12@2/1
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 93% • 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 • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.113.196.254, 13.107.3.254, 13.64.90.137, 52.255.188.83, 13.88.21.125, 51.104.139.180, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247, 13.107.43.13, 13.107.43.12, 20.190.160.6, 20.190.160.75, 20.190.160.69, 20.190.160.134, 20.190.160.132, 20.190.160.71, 20.190.160.73, 20.190.160.136, 51.11.168.232 • Excluded domains from analysis (whitelisted): odc-web-brs.onedrive.akadns.net, odc-dm-files-geo.onedrive.akadns.net, arc.msn.com.nsatc.net, s-ring.msedge.net, www.tm.lg.prod.aadmsa.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, l-0004.dc-msedge.net, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, teams-9999.teams-msedge.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, odc-dm-files.onedrive.akadns.net.l-0003.dc-msedge.net.l-0003.l-msedge.net, ams2.next.a.prd.aadg.trafficmanager.net, login.live.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, odc-dm-files-brs.onedrive.akadns.net, odc-web-geo.onedrive.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, l-0003.dc-msedge.net, settings-win.data.microsoft.com, s-ring.s-9999.s-msedge.net, login.msa.msidentity.com, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, s-9999.s-msedge.net, blobcollector.events.data.trafficmanager.net, teams-ring.teams-9999.teams-msedge.net, teams-ring.msedge.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/357184/sample/V33QokMrIv.exe

Simulations

Behavior and APIs

Time	Type	Description
09:26:25	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\subfolder1\filename1.exe
09:26:29	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe" s>$(Arg0)
09:26:29	API Interceptor	666x Sleep call for process: RegAsm.exe modified

Time	Type	Description
09:26:30	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
09:26:33	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
09:26:41	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
194.5.98.202	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	3Fv4j323nj.exe	Get hash	malicious	Browse	• 194.5.98.182
	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

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	3Fv4j323nj.exe	Get hash	malicious	Browse	
	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	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	

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: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: 3Fv4j323nj.exe, Detection: malicious, Browse • 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
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**

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegAsm.exe.log	
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\tmp7CFF.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\tmp801C.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\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	928
Entropy (8bit):	7.024371743172393

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Encrypted:	false
SSDEEP:	24:IQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtw:Ik/lCrwfk/lCrwfk/lCrwfk/lCrw8
MD5:	CCB690520E68EE385ACC0ACFE759AFFC
SHA1:	33F0DA3F55E5B3C5AC19B61D31471CB60BCD5C96
SHA-256:	166154225DAB5FCB79C1CA97D371B159D37B83FBC0ADABCD8EBA98FA113A7A3B
SHA-512:	AC4F3CF1F8F460745D37E6350861C2FBCDDCC1BBDE0A48FB361BFBF5B1EBF10A05F798A72CE413FCA073FF8108955353DDBCBD9D50CED6CDAE231C67A28F DA3
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.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.....&.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.....&.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:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:zTn:zTn
MD5:	92E49A758034CCCB53F7E0C2540D8D1F
SHA1:	A110CF375A1151871163162E42572DB30665F4DD
SHA-256:	C7CB3AE57F1E7A86EDD4CBBB313AB5E1BDF253C6205AB1B2188DD27F44C6D11C
SHA-512:	376B05470948B965687BD787F2FF2A81B62F2D3157FD9213DD2D885453FE05FBFB0E6B4EF3F71774B6CA1A9AEE215DA5756F3E679C075B89D112E9225D055128
Malicious:	**true**
Preview:	3YR...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:	69B2B0AB1A6E13395EF52DCB903B8E17D842E6D0D44F801FF2659CFD5EC343C8CC57928B02961FC7099AD43FF05633BAF5AC39042A00C8676D4FA8F6F8C2A5 7
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):	4.886067635976852
Encrypted:	false
SSDEEP:	1536:uWWTwV4fVhuoUaaAAwT4uv65YEWDTkIlmak5AEivuxVQwV4MjW:2wVUPOpUlviYEWnkIlmak5zivQqwV
MD5:	E18DBE57194DD717D54A907BA8E6D3E1
SHA1:	76BACC8C5FBBF675399C39C42565DFC3D77BE98B
SHA-256:	B5D510179AB07F09C10CFA2EA9D95346FB696AFD3F642AF2882B3F4CD16D3FF5
SHA-512:	B5B4064FB475590E7EBFA51857117E5C8DAC0C98402809856CD17CF40EDBF455A28ECAB9BD4B431997C50AC1767AB7724F79ED356C33690AA9CB2DCDF38F79 8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 9%

C:\Users\user\subfolder1\filename1.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1....0...~..0.....0...Rich1.....PE..L....bW.....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:Direc tory 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):	4.886067635976852
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:	V33QokMrIv.exe
File size:	131072
MD5:	e18dbe57194dd717d54a907ba8e6d3e1
SHA1:	76bacc8c5fbbf675399c39c42565dfc3d77be98b
SHA256:	b5d510179ab07f09c10cfa2ea9d95346fb696afd3f642af2882b3f4cd16d3ff5
SHA512:	b5b4064fb475590e7ebfa51857117e5c8dac0c98402809856cd17cf40edbf455a28ecab9bd4b431997c50ac1767ab7724f79ed356c33690aa9cb2dcdf38f7968
SSDEEP:	1536:uWWTwV4fVhuoUaaAAwT4uv65YEWDTkIlmak5AEivuxVQwV4MjW:2wVUPOpUlviYEWnkIlmak5zivQqwV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L....bW.....P.....`....@.....

File Icon

	
Icon Hash:	01d292796dda0080

Static PE Info

General

Entrypoint:	0x4013dc

General

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:	0x57629AC2 [Thu Jun 16 12:25:38 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	cc882d101998a701353b40b0cd8c341a

Entrypoint Preview

Instruction
push 00412778h
call 00007FCC9CB3C453h
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
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
cdq
push edx
movsd
inc esp
pop edi
test al, 15h
inc esp
cdq
das
xchg eax, ecx
mov al, byte ptr [1610F6ADh]
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
xor cl, byte ptr [7061430Ah]
push esi
inc ecx
push edx
inc ebp
push esp
dec edi
inc edi
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
add al, 8Fh
outsd
mov edx, 7A63B091h
inc edi

Instruction
sbb dword ptr [eax+2FFB4570h], FFFFFFC3h
int 7Bh
cdq
adc ch, 00000022h
xchg dword ptr [edx+4Fh], esi
mov bl, 6Ch
out dx, al
xor byte ptr [ecx], al
push es
jle 00007FCC9CB3C3EDh
cmp cl, byte ptr [edi-53h]
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
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
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
mov eax, dword ptr [A5000112h]
jnle 00007FCC9CB3C462h
add byte ptr [eax], al
adc al, byte ptr [eax]
push esp
push ebp
inc edx
inc ebp
push edx
inc ebx
push ebp
dec esp
inc ecx
push esp
dec edi
push ebx
push eax
dec ecx
dec esi
dec edi
push ebp
push ebx
add byte ptr [42000A01h], cl
jne 00007FCC9CB3C4D0h
add byte ptr fs:[eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0x15974	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x17000	0x83f6	.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	0x14da4	0x15000	False	0.404203869048	data	5.57673610906	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	0x83f6	0x9000	False	0.340494791667	data	3.53320400461	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1f2ce	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1dca6	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	0x1bffe	0x1ca8	data		
RT_ICON	0x1b356	0xca8	data		
RT_ICON	0x1afee	0x368	GLS_BINARY_LSB_FIRST		
RT_ICON	0x18a46	0x25a8	data		
RT_ICON	0x1799e	0x10a8	data		
RT_ICON	0x17536	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x174c0	0x76	data		
RT_VERSION	0x17240	0x280	data		

Imports

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

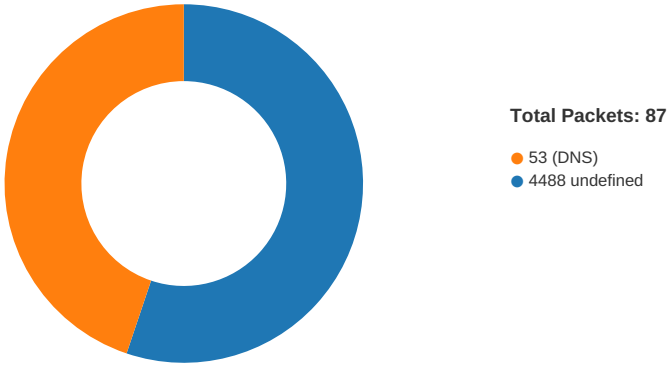
Description	Data
Translation	0x0000 0x04b0
InternalName	KARAKTERISTIKONS
FileVersion	1.00
CompanyName	Sinth Radio
ProductName	Sinth Radio
ProductVersion	1.00
FileDescription	Sinth Radio
OriginalFilename	KARAKTERISTIKONS.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/24/21-09:26:30.194652	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49766	4488	192.168.2.4	194.5.98.202
02/24/21-09:26:36.466553	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49767	4488	192.168.2.4	194.5.98.202
02/24/21-09:26:42.713931	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49768	4488	192.168.2.4	194.5.98.202
02/24/21-09:26:49.051394	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	4488	192.168.2.4	194.5.98.202

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 09:26:29.759485960 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:30.072976112 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:30.073151112 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:30.194652081 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:30.519912004 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:30.520106077 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:30.579900026 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:30.621732950 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:30.817673922 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:30.817770004 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:31.072177887 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:31.072329998 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:31.379748106 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:31.379842043 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:31.865875959 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:31.865948915 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:31.897878885 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:31.897898912 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:31.897965908 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:31.898910046 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:31.898935080 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:31.898964882 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:31.898991108 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:31.900007010 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:31.900026083 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:31.900054932 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:31.900068998 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:31.900100946 CET	49766	4488	192.168.2.4	194.5.98.202

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 09:26:31.900779963 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:31.900842905 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:31.900964975 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:31.900985003 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:31.901024103 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:31.901043892 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.147021055 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.147356033 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.148334980 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.148435116 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.155035973 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.155081987 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.155155897 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.155174017 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.157094955 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.157135010 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.157166004 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.157191038 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.157259941 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.157358885 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.158186913 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.158226013 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.158242941 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.158289909 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.158941984 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.158981085 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.158999920 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.159012079 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.159029007 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.159085035 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.159105062 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.159154892 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.160456896 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.160502911 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.160518885 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.160587072 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.160630941 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.160686016 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.161052942 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.161092043 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.161123991 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.161134958 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.163206100 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.163245916 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.163291931 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.163326979 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.186757088 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.428322077 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.428378105 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.428481102 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.428503990 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.428936958 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.429208994 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.429279089 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.430398941 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.430552959 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.430603981 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.430718899 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.431397915 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.431442976 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.431495905 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.432112932 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.432153940 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.432179928 CET	49766	4488	192.168.2.4	194.5.98.202

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 09:26:32.432225943 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.434156895 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.434190035 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.434241056 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.434262037 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.434284925 CET	4488	49766	194.5.98.202	192.168.2.4
Feb 24, 2021 09:26:32.434326887 CET	49766	4488	192.168.2.4	194.5.98.202
Feb 24, 2021 09:26:32.434345007 CET	4488	49766	194.5.98.202	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 09:24:01.168829918 CET	49714	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:01.217495918 CET	53	49714	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:01.496834040 CET	58028	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:01.545589924 CET	53	58028	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:02.737222910 CET	53097	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:02.789077044 CET	53	53097	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:03.904197931 CET	49257	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:03.954843998 CET	53	49257	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:04.748075962 CET	62389	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:04.799927950 CET	53	62389	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:06.179506063 CET	49910	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:06.228266954 CET	53	49910	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:07.560776949 CET	55854	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:07.622188091 CET	53	55854	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:08.894939899 CET	64549	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:08.949863911 CET	53	64549	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:11.116444111 CET	63153	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:11.166915894 CET	53	63153	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:17.570039988 CET	52991	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:17.618900061 CET	53	52991	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:28.313499928 CET	53700	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:28.365087986 CET	53	53700	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:29.132186890 CET	51726	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:29.184046984 CET	53	51726	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:30.045975924 CET	56794	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:30.095005989 CET	53	56794	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:30.917124033 CET	56534	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:30.967005968 CET	53	56534	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:32.215751886 CET	56627	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:32.267752886 CET	53	56627	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:32.378673077 CET	56621	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:32.427474976 CET	53	56621	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:33.902875900 CET	63116	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:33.951662064 CET	53	63116	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:35.413022995 CET	64078	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:35.465909004 CET	53	64078	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:41.079289913 CET	64801	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:41.127976894 CET	53	64801	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:42.642734051 CET	61721	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:42.692765951 CET	53	61721	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:46.903964043 CET	51255	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:46.955904961 CET	53	51255	8.8.8.8	192.168.2.4
Feb 24, 2021 09:24:59.856170893 CET	61522	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:24:59.931910038 CET	53	61522	8.8.8.8	192.168.2.4
Feb 24, 2021 09:25:00.631495953 CET	52337	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:25:00.732729912 CET	53	52337	8.8.8.8	192.168.2.4
Feb 24, 2021 09:25:01.512803078 CET	55046	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:25:01.581609964 CET	53	55046	8.8.8.8	192.168.2.4
Feb 24, 2021 09:25:02.044190884 CET	49612	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:25:02.101701021 CET	53	49612	8.8.8.8	192.168.2.4
Feb 24, 2021 09:25:02.605772972 CET	49285	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:25:02.663177967 CET	53	49285	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 09:25:03.188625097 CET	50601	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:25:03.251790047 CET	53	50601	8.8.8.8	192.168.2.4
Feb 24, 2021 09:25:03.889224052 CET	60875	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:25:03.937957048 CET	53	60875	8.8.8.8	192.168.2.4
Feb 24, 2021 09:25:04.678129911 CET	56448	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:25:04.744019032 CET	53	56448	8.8.8.8	192.168.2.4
Feb 24, 2021 09:25:05.883210897 CET	59172	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:25:05.946980000 CET	53	59172	8.8.8.8	192.168.2.4
Feb 24, 2021 09:25:06.425657034 CET	62420	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:25:06.499449968 CET	53	62420	8.8.8.8	192.168.2.4
Feb 24, 2021 09:25:06.626337051 CET	60579	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:25:06.692455053 CET	53	60579	8.8.8.8	192.168.2.4
Feb 24, 2021 09:25:14.779095888 CET	50183	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:25:14.838089943 CET	53	50183	8.8.8.8	192.168.2.4
Feb 24, 2021 09:25:42.622454882 CET	61531	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:25:42.673011065 CET	53	61531	8.8.8.8	192.168.2.4
Feb 24, 2021 09:25:46.251863003 CET	49228	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:25:46.320204020 CET	53	49228	8.8.8.8	192.168.2.4
Feb 24, 2021 09:26:25.442338943 CET	59794	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:26:25.502111912 CET	53	59794	8.8.8.8	192.168.2.4
Feb 24, 2021 09:26:26.115159035 CET	55916	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:26:26.206942081 CET	53	55916	8.8.8.8	192.168.2.4
Feb 24, 2021 09:28:59.089103937 CET	52752	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:28:59.142637968 CET	53	52752	8.8.8.8	192.168.2.4
Feb 24, 2021 09:29:00.463768959 CET	60542	53	192.168.2.4	8.8.8.8
Feb 24, 2021 09:29:00.531222105 CET	53	60542	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 09:26:25.442338943 CET	192.168.2.4	8.8.8.8	0x20d9	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Feb 24, 2021 09:26:26.115159035 CET	192.168.2.4	8.8.8.8	0x936	Standard query (0)	ibkebw.dm.files.1drv.com	A (IP address)	IN (0x0001)

DNS Answers

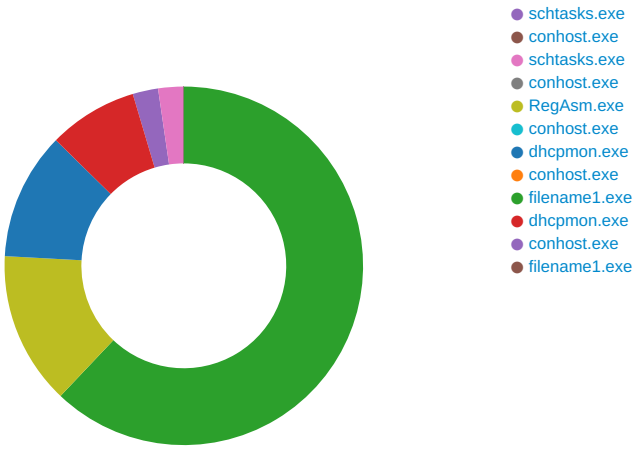
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2021 09:26:25.502111912 CET	8.8.8.8	192.168.2.4	0x20d9	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 09:26:26.206942081 CET	8.8.8.8	192.168.2.4	0x936	No error (0)	ibkebw.dm.files.1drv.com	dm-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 09:26:26.206942081 CET	8.8.8.8	192.168.2.4	0x936	No error (0)	dm-files.fe.1drv.com	odc-dm-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 09:28:59.142637968 CET	8.8.8.8	192.168.2.4	0xf14e	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

- V33QokMrIv.exe
- taskhostw.exe
- RegAsm.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: V33QokMrIv.exe PID: 6352 Parent PID: 5976

General

Start time:	09:24:09
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\V33QokMrIv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\V33QokMrIv.exe'
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	E18DBE57194DD717D54A907BA8E6D3E1
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: taskhostw.exe PID: 6556 Parent PID: 968

General

Start time:	09:24:47
Start date:	24/02/2021
Path:	C:\Windows\System32\taskhostw.exe
Wow64 process (32bit):	false
Commandline:	taskhostw.exe None
Imagebase:	0x7ff73c340000
File size:	87904 bytes
MD5 hash:	CE95E236FC9FE2D6F16C926C75B18BAF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegAsm.exe PID: 6556 Parent PID: 6352

General

Start time:	09:26:10
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\V33QokMrIv.exe'
Imagebase:	0xc00000
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: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.1253583807.000000001EDB3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 0000000F.00000002.1187103126.0000000001002000.00000040.00000001.sdmp, Author: Joe Security
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	1007997	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	10046A9	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	10046A9	InternetOpenUrlA
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	10046A9	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	10046A9	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	10046A9	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	10046A9	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	722760AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	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	200707A1	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	2007089B	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	200707A1	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	20070B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7CFF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	20070D1C	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	2007089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp801C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	20070D1C	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	200707A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	200707A1	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	722760AC	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	722760AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	2007089B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7CFF.tmp	success or wait	1	1DB5BF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp801C.tmp	success or wait	1	1DB5BF0E	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 c2 9a 62 57 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.... $.......u...1...1...1.......0. ..~...0.......0...Rich1....... ....PE..L.....bW............. ...P...................`....@.	success or wait	1	1001D60	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	33 59 52 e1 9d d8 d8 48	3YR....H	success or wait	1	20070A53	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	53248	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 d4 cc 7b 5a 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 a0 00 00 00 20 00 00 00 00 00 00 de b7 00 00 00 20 00 00 00 c0 00 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 01 00 00 10 00 00 4e c1 01 00 03 00 40 05 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......PE..L..... {Z.................... ....@.. ....N.....@.................	success or wait	1	20070B20	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7CFF.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.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	20070A53	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	20070A53	WriteFile
C:\Users\user\AppData\Local\Temp\tmp801C.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	20070A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	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.....&.	success or wait	1	20070A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	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.....&.	success or wait	3	20070A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V33QokMrIv.exe	unknown	131072	success or wait	1	1007997	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7234BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe	unknown	4096	success or wait	1	7234BF06	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe	unknown	512	success or wait	1	7234BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	20070A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	success or wait	1	20070A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	end of file	1	20070A53	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7234BF06	unknown

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	10018F7	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	20070C12	RegSetValueExW

Analysis Process: conhost.exe PID: 5664 Parent PID: 6556

General

Start time:	09:26:11
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 5496 Parent PID: 6556

General

Start time:	09:26:27
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\tmp7CFF.tmp'
Imagebase:	0x920000
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\tmp7CFF.tmp	unknown	2	success or wait	1	92AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7CFF.tmp	unknown	1320	success or wait	1	92ABD9	ReadFile

Analysis Process: conhost.exe PID: 5500 Parent PID: 5496

General

Start time:	09:26:27
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 5516 Parent PID: 6556

General

Start time:	09:26:28
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\tmp801C.tmp'
Imagebase:	0x920000
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\tmp801C.tmp	unknown	2	success or wait	1	92AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp801C.tmp	unknown	1311	success or wait	1	92ABD9	ReadFile

Analysis Process: conhost.exe PID: 6520 Parent PID: 5516

General

Start time:	09:26:28
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 768 Parent PID: 968

General

Start time:	09:26:29
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:	0x150000
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	722760AC	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	722760AC	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	722634A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	85A53F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\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	85A53F	WriteFile
\Device\ConDrv	unknown	0			success or wait	1	85A53F	WriteFile
\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	85A53F	WriteFile
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	7254A33A	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	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	722A5544	unknown

Analysis Process: conhost.exe PID: 6012 Parent PID: 768

General

Start time:	09:26:30
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 2936 Parent PID: 968

General

Start time:	09:26:30
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:	0x740000
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%, 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	722760AC	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	722760AC	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	722634A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	7188DCB3	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	7188DFAB	unknown
\Device\ConDrv	unknown	0			success or wait	1	7188DCB3	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	7188DFAB	unknown

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	7254A33A	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	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown

Analysis Process: conhost.exe PID: 4244 Parent PID: 2936

General

Start time:	09:26:30
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6092 Parent PID: 3424

General

Start time:	09:26:33
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:	E18DBE57194DD717D54A907BA8E6D3E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 9%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: dhcpmon.exe PID: 6896 Parent PID: 3424

General

Start time:	09:26:41
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'
Imagebase:	0x1f0000
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	722760AC	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	722760AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	7188DCB3	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	7188DFAB	unknown
\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	7188DFAB	unknown

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	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown

Analysis Process: conhost.exe PID: 6864 Parent PID: 6896

General

Start time:	09:26:42
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: filename1.exe PID: 6980 Parent PID: 3424

General

Start time:	09:26:50
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:	E18DBE57194DD717D54A907BA8E6D3E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis