ID: 319525
Sample Name: 1kn1ejwPxi.exe
Cookbook: default.jbs
Time: 11:59:23
Date: 18/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

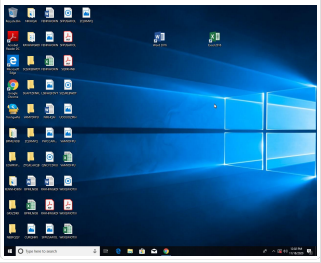
Analysis Report 1kn1ejwPxi.exe

Overview

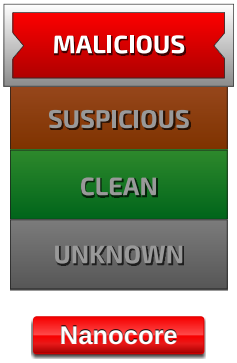
General Information

Sample Name:	1kn1ejwPxi.exe
Analysis ID:	319525
MD5:	d4dc21771af067f..
SHA1:	4eceb759e8ce69..
SHA256:	6e6132e3f3bc119.
Tags:	exe NanoCore nVpn RAT

Most interesting Screenshot:



Detection



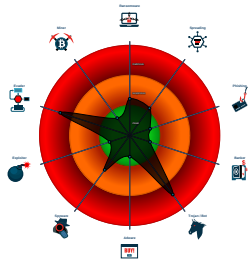
Nanocore

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 doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w10x64**
- 1kn1ejwPxi.exe (PID: 7064 cmdline: 'C:\Users\user\Desktop\1kn1ejwPxi.exe' MD5: D4DC21771AF067F1A4E1BE14A06D9628)
  - 1kn1ejwPxi.exe (PID: 5748 cmdline: C:\Users\user\Desktop\1kn1ejwPxi.exe MD5: D4DC21771AF067F1A4E1BE14A06D9628)
  - 1kn1ejwPxi.exe (PID: 5844 cmdline: C:\Users\user\Desktop\1kn1ejwPxi.exe MD5: D4DC21771AF067F1A4E1BE14A06D9628)
  - 1kn1ejwPxi.exe (PID: 6592 cmdline: C:\Users\user\Desktop\1kn1ejwPxi.exe MD5: D4DC21771AF067F1A4E1BE14A06D9628)
  - 1kn1ejwPxi.exe (PID: 6516 cmdline: C:\Users\user\Desktop\1kn1ejwPxi.exe MD5: D4DC21771AF067F1A4E1BE14A06D9628)
    - schtasks.exe (PID: 6672 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp9EB6.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6932 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6644 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpA1D4.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6636 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- 1kn1ejwPxi.exe (PID: 6632 cmdline: C:\Users\user\Desktop\1kn1ejwPxi.exe 0 MD5: D4DC21771AF067F1A4E1BE14A06D9628)
  - 1kn1ejwPxi.exe (PID: 5340 cmdline: C:\Users\user\Desktop\1kn1ejwPxi.exe MD5: D4DC21771AF067F1A4E1BE14A06D9628)
- vlc.exe (PID: 7148 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: D4DC21771AF067F1A4E1BE14A06D9628)
  - vlc.exe (PID: 5364 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: D4DC21771AF067F1A4E1BE14A06D9628)
  - vlc.exe (PID: 5392 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: D4DC21771AF067F1A4E1BE14A06D9628)
- dhcpmon.exe (PID: 5728 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: D4DC21771AF067F1A4E1BE14A06D9628)
  - dhcpmon.exe (PID: 5568 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: D4DC21771AF067F1A4E1BE14A06D9628)
- dhcpmon.exe (PID: 6212 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: D4DC21771AF067F1A4E1BE14A06D9628)
  - dhcpmon.exe (PID: 5012 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: D4DC21771AF067F1A4E1BE14A06D9628)
- vlc.exe (PID: 6480 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: D4DC21771AF067F1A4E1BE14A06D9628)
  - vlc.exe (PID: 3588 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: D4DC21771AF067F1A4E1BE14A06D9628)
  - vlc.exe (PID: 6940 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: D4DC21771AF067F1A4E1BE14A06D9628)
  - vlc.exe (PID: 6928 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: D4DC21771AF067F1A4E1BE14A06D9628)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "C2: ": [
    "185.140.53.132"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.624204849.00000000071D0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5fee:$x1: NanoCore.ClientPluginHost • 0x602b:$x2: IClientNetworkHost
00000009.00000002.624204849.00000000071D0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5fee:$x2: NanoCore.ClientPluginHost • 0x9441:$s4: PipeCreated • 0x6018:$s5: IClientLoggingHost
0000001B.00000002.530956930.0000000003F49000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001B.00000002.530956930.0000000003F49000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x435cd:$a: NanoCore • 0x43626:$a: NanoCore • 0x43663:$a: NanoCore • 0x436dc:$a: NanoCore • 0x56d87:$a: NanoCore • 0x56d9c:$a: NanoCore • 0x56dd1:$a: NanoCore • 0x6fd73:$a: NanoCore • 0x6fd88:$a: NanoCore • 0x6fdbd:$a: NanoCore • 0x4362f:$b: ClientPlugin • 0x4366c:$b: ClientPlugin • 0x43f6a:$b: ClientPlugin • 0x43f77:$b: ClientPlugin • 0x56b43:$b: ClientPlugin • 0x56b5e:$b: ClientPlugin • 0x56b8e:$b: ClientPlugin • 0x56da5:$b: ClientPlugin • 0x56dda:$b: ClientPlugin • 0x6fb2f:$b: ClientPlugin • 0x6fb4a:$b: ClientPlugin
00000012.00000002.509910009.000000000040E1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x146bd:$x1: NanoCore.ClientPluginHost • 0x146fa:$x2: IClientNetworkHost • 0x1822d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 137 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.1kn1ejwPxi.exe.7130000.12.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2205:$x1: NanoCore.ClientPluginHost • 0x223e:$x2: IClientNetworkHost
9.2.1kn1ejwPxi.exe.7130000.12.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2205:$x2: NanoCore.ClientPluginHost • 0x2320:$s4: PipeCreated • 0x221f:$s5: IClientLoggingHost
9.2.1kn1ejwPxi.exe.7150000.14.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x39eb:$x1: NanoCore.ClientPluginHost • 0x3a24:$x2: IClientNetworkHost
9.2.1kn1ejwPxi.exe.7150000.14.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x39eb:$x2: NanoCore.ClientPluginHost • 0x3b36:$s4: PipeCreated • 0x3a05:$s5: IClientLoggingHost
9.2.1kn1ejwPxi.exe.7100000.9.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x16e3:$x1: NanoCore.ClientPluginHost • 0x171c:$x2: IClientNetworkHost
Click to see the 71 entries				

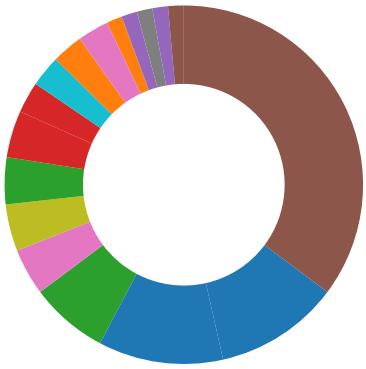
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

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

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- .NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

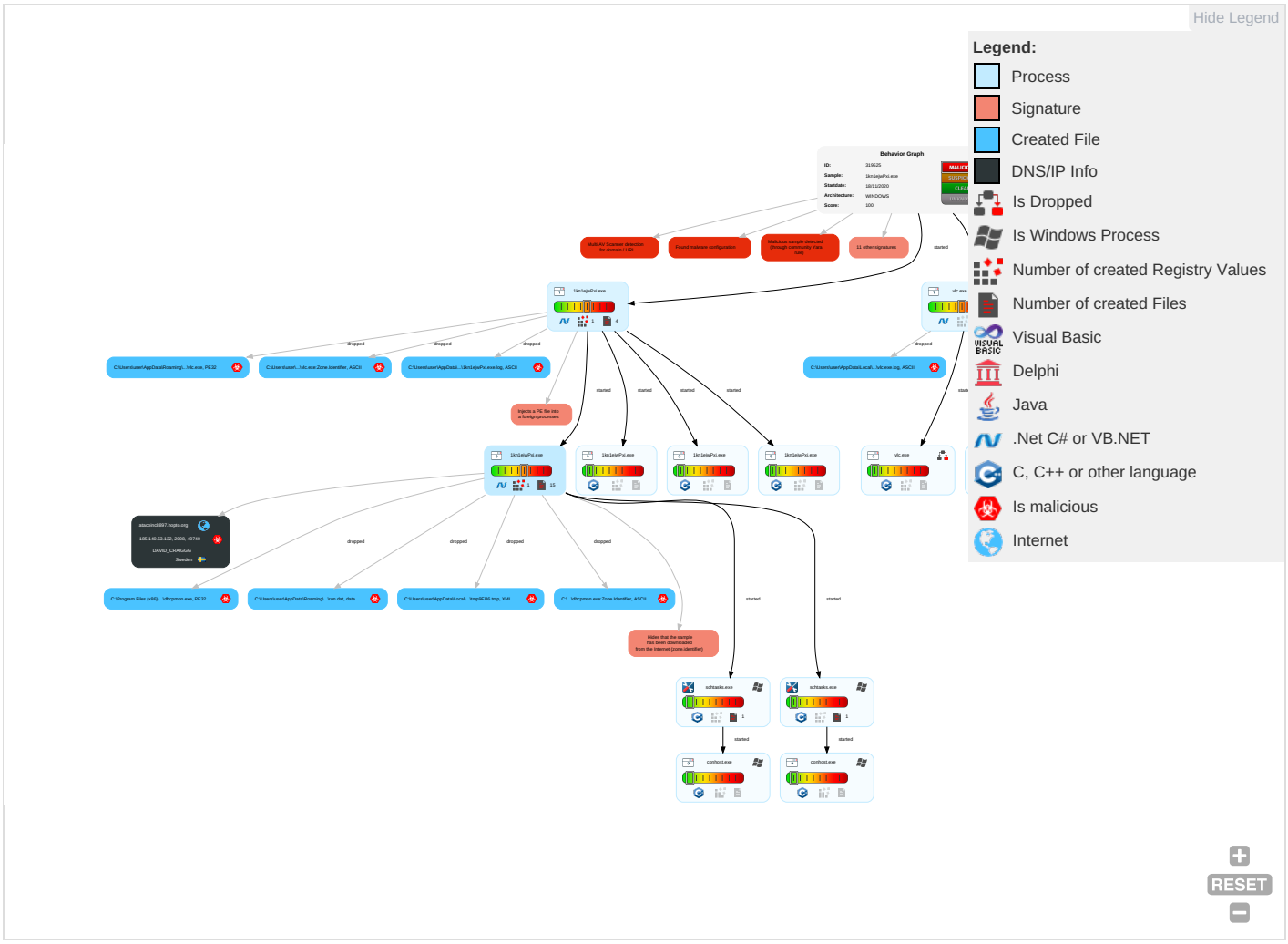
Detected Nanocore Rat

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
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	Input Capture 2 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Registry Run Keys / Startup Folder 1 1	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1 1	Obfuscated Files or Information 1	Security Account Manager	System Information Discovery 1 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 1	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

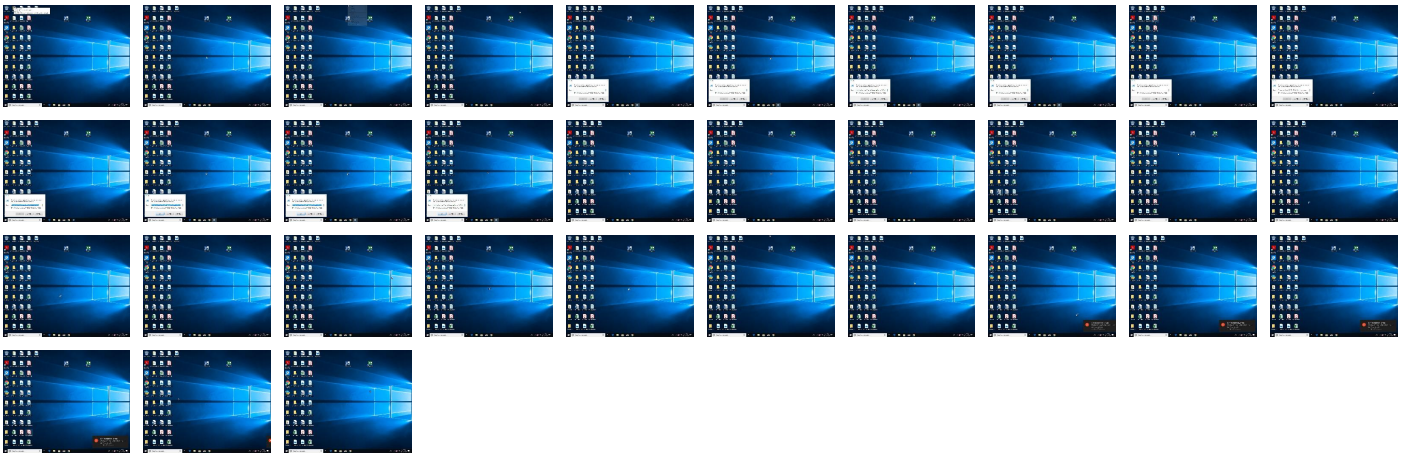
Behavior Graph



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
1kn1ejwPxi.exe	17%	Virustotal		Browse
1kn1ejwPxi.exe	48%	ReversingLabs	ByteCode-MSIL.Trojan.Injuke	
1kn1ejwPxi.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	17%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	48%	ReversingLabs	ByteCode-MSIL.Trojan.Injuke	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	17%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	48%	ReversingLabs	ByteCode-MSIL.Trojan.Injuke	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
25.2.1kn1ejwPxi.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
35.2.vlc.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
27.2.vlc.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
28.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
30.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.1kn1ejwPxi.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
atacoinc8897.hopto.org	6%	Virustotal		Browse

URLs

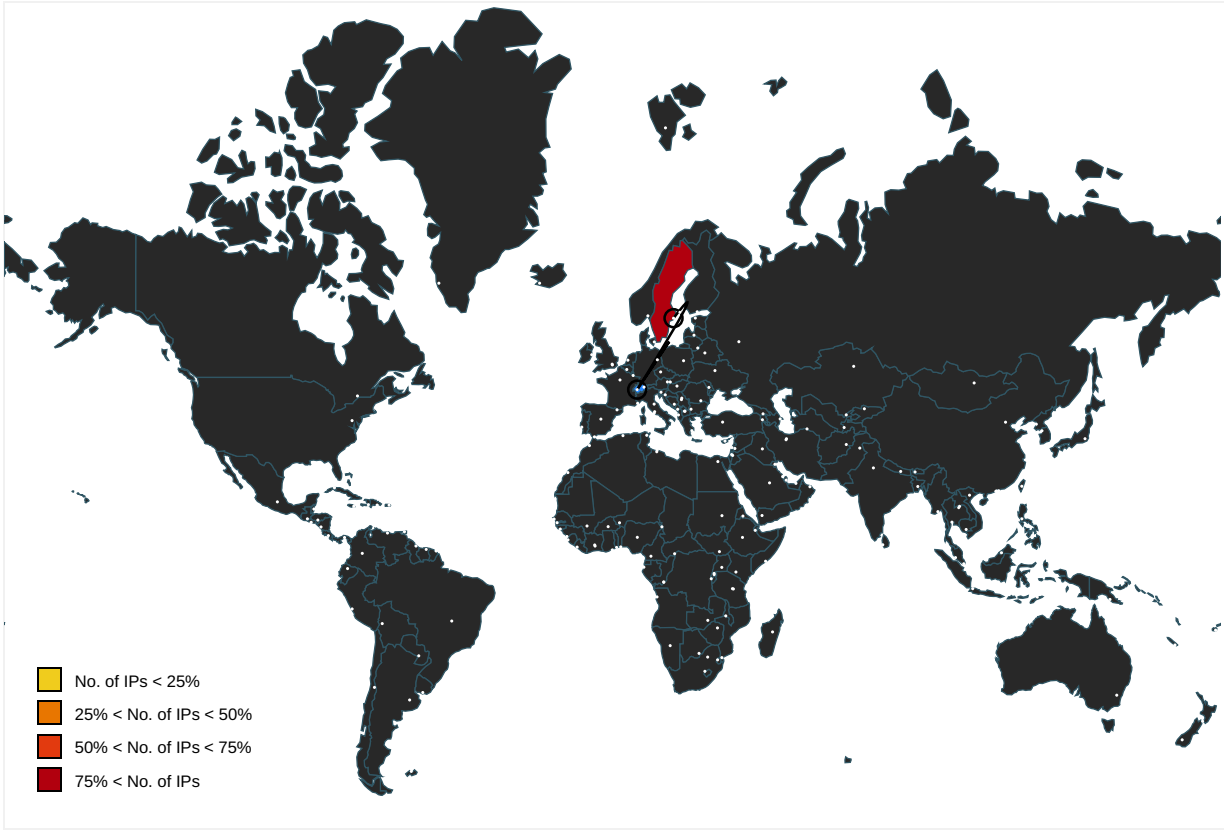
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
atacoinc8897.hopto.org	185.140.53.132	true	true	• 6%, Virustotal, Browse	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.132	unknown	Sweden		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	319525
Start date:	18.11.2020
Start time:	11:59:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1kn1ejwPxi.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:	38
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@36/14@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.8% (good quality ratio 1.1%) • Quality average: 45.3% • Quality standard deviation: 40.9%
HCA Information:	• Successful, ratio: 84% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 51.104.144.132, 52.155.217.156, 20.54.26.129, 8.248.113.254, 8.253.95.120, 67.26.137.254, 67.27.234.126, 67.27.233.254, 52.242.211.89, 92.122.213.194, 92.122.213.247, 23.210.248.85 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, americas1.notify.windows.com.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, dm3p.wns.notify.windows.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:01:01	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run vlc "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"
12:01:07	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\1kn1ejwPxi.exe" s>$(Arg0)
12:01:08	API Interceptor	707x Sleep call for process: 1kn1ejwPxi.exe modified
12:01:09	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
12:01:10	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
12:01:18	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run vlc "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.132	7iatifHQEp.exe	Get hash	malicious	Browse	
	Do43p0ghpz.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	zWKtabs92B.exe	Get hash	malicious	Browse	
	0076364_00533MXS2.jar	Get hash	malicious	Browse	
	Atlas Home Products Inc RFQ_pdf.jar	Get hash	malicious	Browse	
	Payment Advice Hsbc_pdf.jar	Get hash	malicious	Browse	
	NOTIFICA DI ARRIVO DHL_PDF.jar	Get hash	malicious	Browse	
	NOTIFICA DI ARRIVO DHL_PDF.jar	Get hash	malicious	Browse	
	BOLDROCCHI SRL ITALY QUOTATION REQUEST_PDF.jar	Get hash	malicious	Browse	
	REQUEST FOR QUOTATION.jar	Get hash	malicious	Browse	
	REQUEST FOR QUOTATION_pdf.jar	Get hash	malicious	Browse	
	REQUEST FOR QUOTATION_pdf.jar	Get hash	malicious	Browse	
	Yasuda Kogyo Thailand Co Ltd Request For Quotation_pdf.jar	Get hash	malicious	Browse	
	Yasuda Kogyo Thailand Co Ltd Request For Quotation_pdf.jar	Get hash	malicious	Browse	
	Ziraat Bankasi Swift_pdf.jar	Get hash	malicious	Browse	
	YI SHNUFA REQUEST FOR QUOTATION.jar	Get hash	malicious	Browse	
	YI SHNUFA REQUEST FOR QUOTATION.jar	Get hash	malicious	Browse	
	TyRSrOojgV.exe	Get hash	malicious	Browse	
	2KGU6Ue1fD.exe	Get hash	malicious	Browse	
	DvYWRCSr5w.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
atacoinc8897.hopto.org	7iatifHQEp.exe	Get hash	malicious	Browse	• 185.140.53.132
	Do43p0ghpz.exe	Get hash	malicious	Browse	• 185.140.53.132
	zWKtabs92B.exe	Get hash	malicious	Browse	• 185.140.53.132
	wIeFid8p7Q.exe	Get hash	malicious	Browse	• 103.125.189.164
	gSTnUDrWFe.exe	Get hash	malicious	Browse	• 185.244.26.199
	FpK385nmHk.exe	Get hash	malicious	Browse	• 185.244.26.199
	7sbXVpHq6E.exe	Get hash	malicious	Browse	• 185.244.26.199
	Z08LsyTAN6.exe	Get hash	malicious	Browse	• 103.125.189.164
	oIgeDSRrq4.exe	Get hash	malicious	Browse	• 23.105.131.174
	OGKH8KZq2Z.exe	Get hash	malicious	Browse	• 23.105.131.174
	INVOICE.doc	Get hash	malicious	Browse	• 23.105.131.174

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	D6vy84I7rJ.exe	Get hash	malicious	Browse	• 185.140.53.149
	7iatifHQEp.exe	Get hash	malicious	Browse	• 185.140.53.132
	Sbext4ZNBq.exe	Get hash	malicious	Browse	• 185.140.53.197
	xEdiPz1bC3.exe	Get hash	malicious	Browse	• 185.140.53.234
	7D1wvBrRib.exe	Get hash	malicious	Browse	• 185.140.53.234
	O8LDCTOK07.exe	Get hash	malicious	Browse	• 185.140.53.233
	aE78QTkV5H.exe	Get hash	malicious	Browse	• 185.244.30.98
	DHL Shipment Notice of Arrival AWB 8032697940773.js	Get hash	malicious	Browse	• 185.165.153.158
	ORDER-#00654.doc.....exe	Get hash	malicious	Browse	• 185.165.153.116
	SMJshb9rCD.exe	Get hash	malicious	Browse	• 185.140.53.154
	vUQV0nqjYx.exe	Get hash	malicious	Browse	• 185.140.53.182
	Do43p0ghpz.exe	Get hash	malicious	Browse	• 185.140.53.132
	DHL ShipmentDHL Shipment 237590.pdf.exe	Get hash	malicious	Browse	• 185.140.53.207
	7GAi7ZFQz8.exe	Get hash	malicious	Browse	• 185.165.153.116
	KL0DeoXZFx.dll	Get hash	malicious	Browse	• 91.193.75.78
	C1jkp1o3Vl.dll	Get hash	malicious	Browse	• 185.140.53.152
	fYRqcuLMYk.exe	Get hash	malicious	Browse	• 185.140.53.137
	02oBhZg39b.exe	Get hash	malicious	Browse	• 185.244.30.112
	7crYMLdmCL.exe	Get hash	malicious	Browse	• 185.140.53.234
	Sw4rkFUNJt.exe	Get hash	malicious	Browse	• 185.140.53.137

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\1kn1ejwPxi.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1124864
Entropy (8bit):	5.014957066819657
Encrypted:	false
SSDEEP:	24576:9tIuv5vRwaAQmDmHKmbQPVU7wKFGhFFfalCb:7Cb
MD5:	D4DC21771AF067F1A4E1BE14A06D9628
SHA1:	4ECEB759E8CE69E05BF0D4F634273AE9768B5561
SHA-256:	6E6132E3F3BC119ADAC878BA65475B581698E8DD7D2169F984BB5EB232F6B3C6
SHA-512:	94503DE5B1ECDE76A041ABC92BEA16D6B950FA930221DC6D03909E0BA9A5404EC8D005CCDE96A15AAA1EECFA7B7EE7A736FED18E87C6A9CE95100D3C0873A95
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 17%, Browse • Antivirus: ReversingLabs, Detection: 48%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....n..... .....@.. ..@.....K.....k.....`..... ..... ..H.....text..... ..... ..`.rsrc....k.....l.....@..@.reloc.....`. .....(.....@..B.....H.....p.....*....)..m.....0..~.....(.... ....:...&8....8.....E.....8...../...&&8....(....o.....:&...&&8....8....8....*8 ....}....8....8....}....8.....0.....8g.....E.....8....8h...8.....@....8P...*.....:...&8....(....8....8.... ....(....9...& ....8....{....:....&8....8.....;....8....8.....8y.....0..5.....0..... {.....:a...&85.....E.....5...E...8.....}

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

Process:	C:\Users\user\Desktop\1kn1ejwPxi.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\1kn1ejwPxi.exe.log

Process:	C:\Users\user\Desktop\1kn1ejwPxi.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADDD
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\1kn1ejwPxi.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD D
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vlc.exe.log	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD D
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp9EB6.tmp	
Process:	C:\Users\user\Desktop\1kn1ejwPxi.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1303
Entropy (8bit):	5.097952448531751
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0VrCxtn:cbk4oL600QydbQxIYODOLedq3OCj
MD5:	DEB3C4FE3C73644F4693F8CD3F075ED1
SHA1:	B17C69EE16AEFCACDC3210BFBF0DC3AA20774590
SHA-256:	8BF64C6CA969DC068BFAC950805FE4E5916B1943094E4A1D3779EE98984EE2F4
SHA-512:	A2695226D6C97C635FA7972E0E94A3266F4E85C82FA9C5ECD01216F0123DBE04765024812DB87EBFA3854D32804D7EFEB92ABB030A22EB9136201230D5F7E13F
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\tmpA1D4.tmp	
Process:	C:\Users\user\Desktop\1kn1ejwPxi.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\tmpA1D4.tmp	
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\1kn1ejwPxi.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKgmR7kkmefoeLBizbCuVkqYM:X4LDAnybgCFcps0OafmCYDlizZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005
SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF385 1
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+ .2e'..E?.G.....[.&

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\1kn1ejwPxi.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:wyt:w+
MD5:	80F3BBD5E455819033C15E691DE356B9
SHA1:	75EA88C2C4A5743BA493C63C581A954F1D600FD7
SHA-256:	89DCB57B299D5227C530A791E6D8CDFD25E3C340050A6D945DF309243EF7C0B6
SHA-512:	2C6BCC416B2A54ED05DED91253CA1BCC36C345AF3B7714665B82B8C7A93CE77BDD9E8BE94871F12D445C2B697F08F4BF37E0D4B07F7E3D5DF8FFC1B69A45D 6E
Malicious:	**true**
Preview:	.....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\1kn1ejwPxi.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\1kn1ejwPxi.exe
File Type:	data
Category:	dropped
Size (bytes):	327768
Entropy (8bit):	**7.999367066417797**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3PlZmqze1d1wl8lkWmtjJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C3A
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i..........J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&.jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\1kn1ejwPxi.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	40
Entropy (8bit):	4.034183719779189
Encrypted:	false
SSDEEP:	3:oNN2+WUdNdA:oNN2RUK
MD5:	8B56B1D61728357BA8AA5BEC389367D9
SHA1:	830F108D36C01F2E425FE4CFBE582299EF9D6A6C
SHA-256:	B2087C20A7C51D5BE7AF38C145426D6622483EED3B864A9594234F4E01FB42C3
SHA-512:	0A9318BDCB81E07B52C4C92E263B9CB4DBD4CCFC98570D40183DA1EA77C7BD2C535B9D07D0125D4F4935B1685AFBC0F83B146842E1DD3C3EF193BDA421C916F
Malicious:	false
Preview:	C:\Users\user\Desktop\1kn1ejwPxi.exe

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	
Process:	C:\Users\user\Desktop\1kn1ejwPxi.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1124864
Entropy (8bit):	5.014957066819657
Encrypted:	false
SSDEEP:	24576:9tIuv5vRwaAQmDmHKmbQPVU7wKFGhFFfalCb:7Cb
MD5:	D4DC21771AF067F1A4E1BE14A06D9628
SHA1:	4ECEB759E8CE69E05BF0D4F634273AE9768B5561
SHA-256:	6E6132E3F3BC119ADAC878BA65475B581698E8DD7D2169F984BB5EB232F6B3C6
SHA-512:	94503DE5B1ECDE76A041ABC92BEA16D6B950FA930221DC6D03909E0BA9A5404EC8D005CCDE96A15AAA1EECFA7B7EE7A736FED18E87C6A9CE95100D3C0873A95
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 17%, Browse • Antivirus: ReversingLabs, Detection: 48%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....n..... .....@.. ....@.....K.....k.....` ..... ..H.....text..... ..... ..`.rsrc....k.....l.....@..@.reloc.....`. .....(.....@..B.....H.....p.....*....)..m.....0..~.....(.... ....:....&8....8.....E.....8.....:/...&&8.....(....o.....:&...&&8....8....8....*8 ....}....8....8....}....8.....0.....8g.....E.....8....8h...8.....@....8P...*.....:....&8.....(....8....8.... ....(....9....& ....8.....{....:....&8.....8.....;....8....8.....8y.....0..5.....0..... {.....:a...&85.....E.....5...E...8.....}

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\1kn1ejwPxi.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe:Zone.Identifier	
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.014957066819657
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	1kn1ejwPxi.exe
File size:	1124864
MD5:	d4dc21771af067f1a4e1be14a06d9628
SHA1:	4eceb759e8ce69e05bf0d4f634273ae9768b5561
SHA256:	6e6132e3f3bc119adac878ba65475b581698e8dd7d2169984bb5eb232f6b3c6
SHA512:	94503de5b1ecde76a041abc92bea16d6b950fa930221dc6d03909e0ba9a5404ec8d005ccde96a15aaa1eecfa7b7ee7a736fed18e87c6a9ce95100d3c08733a95
SSDEEP:	24576:9tIuv5vRwaAQmDmHKmbQPVU7wKFGhFFfalCb:7Cb
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....n..... .....@.. .....@.....

File Icon

Icon Hash:	74f2dbb284c2e2ee

Static PE Info

General

Entrypoint:	0x4cd8de
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FB3FA82 [Tue Nov 17 16:29:54 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4

General	
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
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
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
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
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xcd890	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xce000	0x46be4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x116000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xcb8e4	0xcba00	False	0.430274996163	data	4.32205844238	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xce000	0x46be4	0x46c00	False	0.198180073984	data	4.61906006707	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x116000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xce1f0	0x42028	dBase IV DBT, blocks size 0, block length 8192, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x110218	0x25a8	data		
RT_ICON	0x1127c0	0x10a8	data		
RT_ICON	0x113868	0x988	data		
RT_ICON	0x1141f0	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x114658	0x4c	data		
RT_VERSION	0x1146a4	0x33c	data		
RT_MANIFEST	0x1149e0	0x204	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators		

Imports

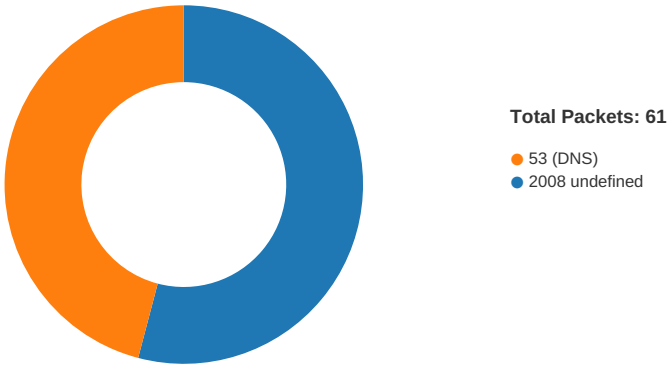
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	(c) 2020 Skype and/or Microsoft
Assembly Version	8.61.0.87
InternalName	POP.exe
FileVersion	8.61.0.87
CompanyName	Skype Technologies S.A.
Comments	Skype Setup
ProductName	Skype
ProductVersion	8.61.0.87
FileDescription	Skype Setup
OriginalFilename	POP.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 12:01:02.598510027 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:02.816780090 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:02.817050934 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:03.231194019 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:03.461755991 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:03.471434116 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:03.689759016 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:03.689866066 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:03.959105015 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:03.959363937 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.228116989 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.247689009 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.247811079 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.247853041 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.247919083 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.248080015 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.248703957 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.468553066 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.468595028 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.468792915 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.468837023 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.468871117 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.469089031 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.469877958 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.469913960 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.469935894 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.470062017 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.470230103 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.470335960 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.695698023 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.695741892 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.695765972 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.695813894 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.695837975 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.695863962 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.695887089 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.695909023 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.695913076 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.695934057 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.695943117 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.695950985 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.695961952 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.695986986 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.696012974 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.696019888 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.696044922 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.696062088 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.696070910 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.696095943 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.696118116 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.696135998 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.696202040 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.918458939 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.918520927 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.918543100 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.918562889 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.918586969 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.918608904 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.918623924 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.918731928 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.918756008 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.918770075 CET	49740	2008	192.168.2.6	185.140.53.132

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 12:01:04.918781042 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.918803930 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.918870926 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.918880939 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.919102907 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919128895 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919152021 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919173002 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919197083 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919219017 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919229031 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.919243097 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919267893 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919290066 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919290066 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.919315100 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919337988 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919339895 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.919363976 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919385910 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919394016 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.919409037 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919431925 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919456005 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919460058 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.919481039 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919485092 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.919504881 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919506073 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.919554949 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919591904 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919601917 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:04.919647932 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:04.919677973 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:05.063699961 CET	49740	2008	192.168.2.6	185.140.53.132
Nov 18, 2020 12:01:05.136939049 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:05.136982918 CET	2008	49740	185.140.53.132	192.168.2.6
Nov 18, 2020 12:01:05.137006998 CET	2008	49740	185.140.53.132	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 12:00:13.248363018 CET	58336	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:00:13.283672094 CET	53	58336	8.8.8.8	192.168.2.6
Nov 18, 2020 12:00:14.335647106 CET	53781	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:00:14.362818956 CET	53	53781	8.8.8.8	192.168.2.6
Nov 18, 2020 12:00:15.164990902 CET	54064	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:00:15.192244053 CET	53	54064	8.8.8.8	192.168.2.6
Nov 18, 2020 12:00:16.190414906 CET	52811	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:00:16.226067066 CET	53	52811	8.8.8.8	192.168.2.6
Nov 18, 2020 12:00:22.570188046 CET	55299	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:00:22.605942965 CET	53	55299	8.8.8.8	192.168.2.6
Nov 18, 2020 12:00:23.417960882 CET	63745	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:00:23.445033073 CET	53	63745	8.8.8.8	192.168.2.6
Nov 18, 2020 12:00:25.078023911 CET	50055	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:00:25.105062008 CET	53	50055	8.8.8.8	192.168.2.6
Nov 18, 2020 12:00:25.993100882 CET	61374	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:00:26.020191908 CET	53	61374	8.8.8.8	192.168.2.6
Nov 18, 2020 12:00:26.873503923 CET	50339	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:00:26.900569916 CET	53	50339	8.8.8.8	192.168.2.6
Nov 18, 2020 12:00:40.930696011 CET	63307	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:00:40.957848072 CET	53	63307	8.8.8.8	192.168.2.6
Nov 18, 2020 12:00:58.304928064 CET	49694	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:00:58.340606928 CET	53	49694	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 12:00:58.967941999 CET	54982	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:00:59.003626108 CET	53	54982	8.8.8.8	192.168.2.6
Nov 18, 2020 12:00:59.488626957 CET	50010	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:00:59.524243116 CET	53	50010	8.8.8.8	192.168.2.6
Nov 18, 2020 12:00:59.890418053 CET	63718	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:00:59.926162004 CET	53	63718	8.8.8.8	192.168.2.6
Nov 18, 2020 12:01:00.538958073 CET	62116	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:01:00.566036940 CET	53	62116	8.8.8.8	192.168.2.6
Nov 18, 2020 12:01:00.776721954 CET	63816	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:01:00.803774118 CET	53	63816	8.8.8.8	192.168.2.6
Nov 18, 2020 12:01:01.035347939 CET	55014	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:01:01.070774078 CET	53	55014	8.8.8.8	192.168.2.6
Nov 18, 2020 12:01:01.243684053 CET	62208	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:01:01.270833015 CET	53	62208	8.8.8.8	192.168.2.6
Nov 18, 2020 12:01:01.667543888 CET	57574	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:01:01.694413900 CET	53	57574	8.8.8.8	192.168.2.6
Nov 18, 2020 12:01:02.519939899 CET	51818	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:01:02.559106112 CET	53	51818	8.8.8.8	192.168.2.6
Nov 18, 2020 12:01:03.119750977 CET	56628	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:01:03.157656908 CET	53	56628	8.8.8.8	192.168.2.6
Nov 18, 2020 12:01:04.055767059 CET	60778	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:01:04.091257095 CET	53	60778	8.8.8.8	192.168.2.6
Nov 18, 2020 12:01:04.437027931 CET	53799	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:01:04.477509022 CET	53	53799	8.8.8.8	192.168.2.6
Nov 18, 2020 12:01:05.111198902 CET	54683	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:01:05.151900053 CET	53	54683	8.8.8.8	192.168.2.6
Nov 18, 2020 12:01:16.582643032 CET	59329	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:01:16.619678020 CET	53	59329	8.8.8.8	192.168.2.6
Nov 18, 2020 12:01:44.567858934 CET	64021	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:01:44.603383064 CET	53	64021	8.8.8.8	192.168.2.6
Nov 18, 2020 12:01:49.293688059 CET	56129	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:01:49.320830107 CET	53	56129	8.8.8.8	192.168.2.6
Nov 18, 2020 12:01:52.468095064 CET	58177	53	192.168.2.6	8.8.8.8
Nov 18, 2020 12:01:52.495204926 CET	53	58177	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 18, 2020 12:01:02.519939899 CET	192.168.2.6	8.8.8.8	0xb57f	Standard query (0)	atacoinc8897.hopto.org	A (IP address)	IN (0x0001)

DNS Answers

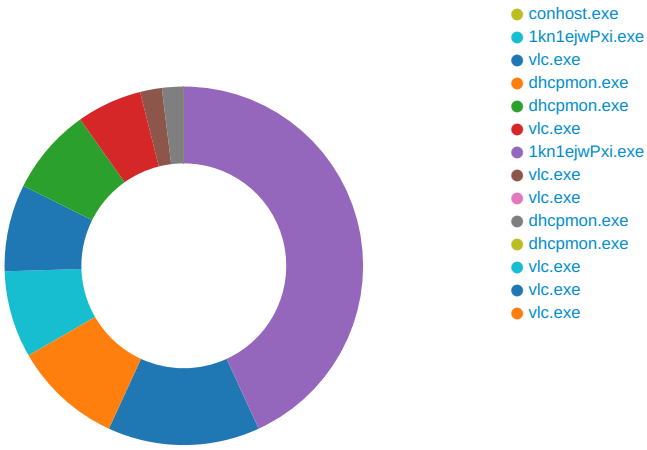
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 18, 2020 12:01:02.559106112 CET	8.8.8.8	192.168.2.6	0xb57f	No error (0)	atacoinc8897.hopto.org		185.140.53.132	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

- 1kn1ejwPxi.exe
- 1kn1ejwPxi.exe
- 1kn1ejwPxi.exe
- 1kn1ejwPxi.exe
- 1kn1ejwPxi.exe
- schtasks.exe
- conhost.exe
- schtasks.exe



Click to jump to process

System Behavior

Analysis Process: 1kn1ejwPxi.exe PID: 7064 Parent PID: 244

General

Start time:	12:00:30
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\1kn1ejwPxi.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\1kn1ejwPxi.exe'
Imagebase:	0xc00000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
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: 00000000.00000002.428049069.00000000042C5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.428049069.00000000042C5000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.428049069.00000000042C5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.427594239.0000000004201000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.427594239.0000000004201000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.427594239.0000000004201000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF1BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.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	5B7B893	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	5B7B893	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\1kn1ejwPxi.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3DC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 82 fa b3 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 ba 0c 00 00 6e 04 00 00 00 00 00 de d8 0c 00 00 20 00 00 00 e0 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 11 00 00 02 00 00 00 00 00 00 02 00 40 85 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......_.......... ....n........... ....@.. ....@................	success or wait	5	5B7B893	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	5B7B893	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\1kn1ejwPxi.exe.log	unknown	425	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0	success or wait	1	6E3DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	vlc	unicode	"C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"	success or wait	1	6CF1646A	RegSetValueExW

Analysis Process: 1kn1ejwPxi.exe PID: 5748 Parent PID: 7064

General

Start time:	12:01:01
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\1kn1ejwPxi.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\1kn1ejwPxi.exe
Imagebase:	0x170000
File size:	1124864 bytes

MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 1kn1ejwPxi.exe PID: 5844 Parent PID: 7064

General

Start time:	12:01:02
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\1kn1ejwPxi.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\1kn1ejwPxi.exe
Imagebase:	0x280000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 1kn1ejwPxi.exe PID: 6592 Parent PID: 7064

General

Start time:	12:01:02
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\1kn1ejwPxi.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\1kn1ejwPxi.exe
Imagebase:	0x240000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 1kn1ejwPxi.exe PID: 6516 Parent PID: 7064

General

Start time:	12:01:03
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\1kn1ejwPxi.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\1kn1ejwPxi.exe
Imagebase:	0xa20000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
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: 00000009.00000002.624204849.00000000071D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source:

00000009.00000002.624204849.00000000071D0000.00000004.00000001.sdmp, Author: Florian Roth

- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.624040800.0000000007160000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.624040800.0000000007160000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.622024902.00000000054F0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.622024902.00000000054F0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.624092570.0000000007180000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.624092570.0000000007180000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.623866439.0000000007110000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.623866439.0000000007110000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.613039388.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.613039388.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.613039388.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.617006298.0000000002F2D000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.621027784.00000000049D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.620931619.0000000004963000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.620931619.0000000004963000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.622854804.0000000006470000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.622854804.0000000006470000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.622854804.0000000006470000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.623238450.0000000006960000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.623238450.0000000006960000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.623644523.00000000070C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.623644523.00000000070C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.623826686.0000000007100000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.623826686.0000000007100000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.616627338.0000000002EC1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.621144468.0000000004AC4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.621144468.0000000004AC4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: NanoCore, Description: unknown, Source: 00000009.00000003.611686179.0000000004AE5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.624006580.0000000007150000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.624006580.0000000007150000.00000004.00000001.sdmp, Author:

	Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.623969104.0000000007140000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.623969104.0000000007140000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.623897987.0000000007120000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.623897987.0000000007120000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.620462893.0000000003EC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.620462893.0000000003EC1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.623932235.0000000007130000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.623932235.0000000007130000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.624127580.0000000007190000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.624127580.0000000007190000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.620703151.0000000004792000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.620703151.0000000004792000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0CCF06	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	6E0CCF06	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	6CF1BEFF	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	6CF11E60	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	6CF1BEFF	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	6CF1DD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CF1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp9EB6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF17038	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	6CF11E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpA1D4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF17038	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	6CF1BEFF	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	6CF1BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF11E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF11E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF11E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9EB6.tmp	success or wait	1	6CF16A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpA1D4.tmp	success or wait	1	6CF16A95	DeleteFileW
C:\Users\user\Desktop\1kn1ejwPxi.exe:Zone.Identifier	success or wait	1	6CE92935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	1a f2 84 af fc 8b d8 48	.....H	success or wait	1	6CF11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 82 fa b3 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 ba 0c 00 00 6e 04 00 00 00 00 00 de d8 0c 00 00 20 00 00 00 e0 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 11 00 00 02 00 00 00 00 00 00 02 00 40 85 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......_.......... ....n........... ....@.. ....@................	success or wait	5	6CF1DD66	CopyFileW
C:\Program Files (x86)\DHCP Mo nitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CF1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp9EB6.tmp	unknown	1303	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveTo ken</LogonType>	success or wait	1	6CF11B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	40	43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 44 65 73 6b 74 6f 70 5c 31 6b 6e 31 65 6a 77 50 78 69 2e 65 78 65	C:\Users\user\Desktop\1kn 1ejwPxi.exe	success or wait	1	6CF11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA1D4.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.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	6CF11B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 7e 66 1e 47 30 5e c3 a9 dd 96 3b b4 2e 95 a2 57 32 c2 3d 10 b3 ce 4b ca 7e c7 4c cc 9f 15 26 66 8d bb 2e 70 c8 04 1b f8 b7 c2 0f e9 ff e7 0b 10 3a 37 72 48 7d bd be f1 88 0d 2f 48 16 b2 87 06 17 96 4c 8c b6 04 3f b5 f3 04 41 08 4b 07 d1 e5 84 4a 17 3d 38 78 21 19 a1 e1 e4 2b fa 32 65 27 d7 1f 45 3f d9 47 11 9e a7 e7 a8 01 f0 5b 00 26	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i..... S.....}FF.2.. .h..M+.....L.#.X..+.....*.... ~f.G0^....;....W2.=...K.~.L... &f...p.....:7rH}...../H .....L...?...A.K....J.=8x!... .+.2e'..E?.G.....[.&	success or wait	1	6CF11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327768	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wpK .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_...Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6CF11B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6CF11B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E08D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E08D72F	unknown
C:\Users\user\Desktop\1kn1ejwPxi.exe	unknown	4096	success or wait	1	6E08D72F	unknown
C:\Users\user\Desktop\1kn1ejwPxi.exe	unknown	512	success or wait	1	6E08D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6CF1646A	RegSetValueExW

Analysis Process: schtasks.exe PID: 6672 Parent PID: 6516

General

Start time:	12:01:06
Start date:	18/11/2020
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\tmp9EB6.tmp'
Imagebase:	0xf50000
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\tmp9EB6.tmp	unknown	2	success or wait	1	F5AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9EB6.tmp	unknown	1304	success or wait	1	F5ABD9	ReadFile

Analysis Process: conhost.exe PID: 6932 Parent PID: 6672

General

Start time:	12:01:07
Start date:	18/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6644 Parent PID: 6516

General

Start time:	12:01:07
Start date:	18/11/2020
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\tmpA1D4.tmp'
Imagebase:	0xf50000
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\tmpA1D4.tmp	unknown	2	success or wait	1	F5AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA1D4.tmp	unknown	1311	success or wait	1	F5ABD9	ReadFile

Analysis Process: conhost.exe PID: 6636 Parent PID: 6644

General

Start time:	12:01:08
Start date:	18/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 1kn1ejwPxi.exe PID: 6632 Parent PID: 936

General

Start time:	12:01:08
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\1kn1ejwPxi.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\1kn1ejwPxi.exe 0
Imagebase:	0xe30000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
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: 00000011.00000002.507305444.0000000004345000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.507305444.0000000004345000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.507305444.0000000004345000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	object name collision	1	5D8B893	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic write	device	sequential only | non directory file	object name collision	1	5D8B893	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile

Analysis Process: vlc.exe PID: 7148 Parent PID: 3440

General

Start time:	12:01:10
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe'
Imagebase:	0xc20000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.509910009.00000000040E1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.509910009.00000000040E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.509910009.00000000040E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.510414453.00000000041A5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.510414453.00000000041A5000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.510414453.00000000041A5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 17%, Virustotal, Browse • Detection: 48%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vlc.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3DC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vlc.exe.log	unknown	425	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0	success or wait	1	6E3DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile

Analysis Process: dhcpmon.exe PID: 5728 Parent PID: 936

General

Start time:	12:01:10
Start date:	18/11/2020
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xb80000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
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: 00000013.00000002.514905304.0000000004185000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.514905304.0000000004185000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.514905304.0000000004185000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 17%, Virustotal, Browse • Detection: 48%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	object name collision	1	59BB893	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic write	device	sequential only | non directory file	object name collision	1	59BB893	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3DC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	425	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0	success or wait	1	6E3DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile

Analysis Process: dhcpmon.exe PID: 6212 Parent PID: 3440

General

Start time:	12:01:18
Start date:	18/11/2020
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x140000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
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: 00000014.00000002.537565440.0000000003685000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.537565440.0000000003685000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.537565440.0000000003685000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	object name collision	1	4F7B893	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic write	device	sequential only | non directory file	object name collision	1	4F7B893	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile

Analysis Process: vlc.exe PID: 6480 Parent PID: 3440

General

Start time:	12:01:26
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe'
Imagebase:	0xbe0000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
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: 00000017.00000002.552753748.0000000004195000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.552753748.0000000004195000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.552753748.0000000004195000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000002.552372687.00000000040D1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.552372687.00000000040D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.552372687.00000000040D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile

Analysis Process: 1kn1ejwPxi.exe PID: 5340 Parent PID: 6632

General

Start time:	12:01:40
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\1kn1ejwPxi.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\1kn1ejwPxi.exe
Imagebase:	0xf50000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
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: 00000019.00000002.517433157.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.517433157.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.517433157.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.519814493.0000000003311000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.519814493.0000000003311000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.520065528.0000000004319000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.520065528.0000000004319000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: vlc.exe PID: 5364 Parent PID: 7148

General

Start time:	12:01:40
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0x1f0000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vlc.exe PID: 5392 Parent PID: 7148

General

Start time:	12:01:41
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0xa50000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
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: 0000001B.00000002.530956930.0000000003F49000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.530956930.0000000003F49000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000002.521475039.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000002.521475039.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.521475039.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000002.530452666.0000000002F41000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.530452666.0000000002F41000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: dhcpmon.exe PID: 5568 Parent PID: 5728

General

Start time:	12:01:44
Start date:	18/11/2020
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Imagebase:	0x9d0000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
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: 0000001C.00000002.535021401.0000000003EC9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000002.535021401.0000000003EC9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001C.00000002.527634171.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000002.527634171.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000002.527634171.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000002.534348993.0000000002EC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000002.534348993.0000000002EC1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: dhcpmon.exe PID: 5012 Parent PID: 6212

General

Start time:	12:01:50
Start date:	18/11/2020
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xb60000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
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: 0000001E.00000002.546761343.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.546761343.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.546761343.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.551302539.0000000004069000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.551302539.0000000004069000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.551029791.0000000003061000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.551029791.0000000003061000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: vlc.exe PID: 3588 Parent PID: 6480

General

Start time:	12:01:59
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0x1f0000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vlc.exe PID: 6940 Parent PID: 6480

General

Start time:	12:02:00
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0x110000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vlc.exe PID: 6928 Parent PID: 6480

General

Start time:	12:02:01
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0xae0000
File size:	1124864 bytes
MD5 hash:	D4DC21771AF067F1A4E1BE14A06D9628
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: 00000023.00000002.569833415.0000000004069000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000023.00000002.569833415.0000000004069000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000023.00000002.569706588.0000000003061000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000023.00000002.569706588.0000000003061000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000023.00000002.567351430.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000023.00000002.567351430.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000023.00000002.567351430.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Reputation:	low

Disassembly

Code Analysis