ID: 319587
Sample Name:
2AyWKsCvVF.exe
Cookbook: default.jbs
Time: 13:13:26
Date: 18/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

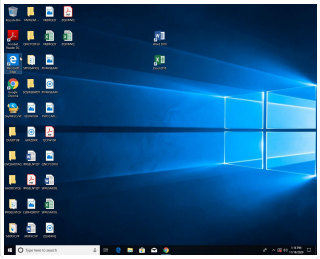
Analysis Report 2AyWKsCvVF.exe

Overview

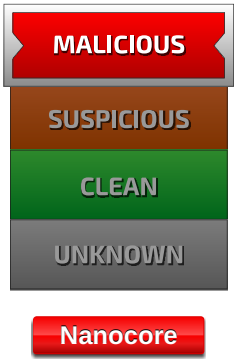
General Information

Sample Name:	2AyWKsCvVF.exe
Analysis ID:	319587
MD5:	678dac5fc4c6a55..
SHA1:	8ea9541292f8e5d.
SHA256:	78491e950a6243..
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection

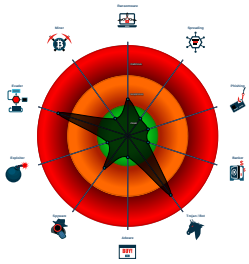


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for 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…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- 2AyWKsCvVF.exe (PID: 6776 cmdline: 'C:\Users\user\Desktop\2AyWKsCvVF.exe' MD5: 678DAC5FC4C6A55F032BA40698895E6A)
  - 2AyWKsCvVF.exe (PID: 6448 cmdline: C:\Users\user\Desktop\2AyWKsCvVF.exe MD5: 678DAC5FC4C6A55F032BA40698895E6A)
    - schtasks.exe (PID: 6924 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp7D39.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6940 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 7116 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp8057.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 7124 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- 2AyWKsCvVF.exe (PID: 5644 cmdline: C:\Users\user\Desktop\2AyWKsCvVF.exe 0 MD5: 678DAC5FC4C6A55F032BA40698895E6A)
  - 2AyWKsCvVF.exe (PID: 5576 cmdline: C:\Users\user\Desktop\2AyWKsCvVF.exe MD5: 678DAC5FC4C6A55F032BA40698895E6A)
  - 2AyWKsCvVF.exe (PID: 5716 cmdline: C:\Users\user\Desktop\2AyWKsCvVF.exe MD5: 678DAC5FC4C6A55F032BA40698895E6A)
  - 2AyWKsCvVF.exe (PID: 4164 cmdline: C:\Users\user\Desktop\2AyWKsCvVF.exe MD5: 678DAC5FC4C6A55F032BA40698895E6A)
- dhcpmon.exe (PID: 6976 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 678DAC5FC4C6A55F032BA40698895E6A)
  - dhcpmon.exe (PID: 5000 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 678DAC5FC4C6A55F032BA40698895E6A)
- vlc.exe (PID: 5720 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: 678DAC5FC4C6A55F032BA40698895E6A)
  - vlc.exe (PID: 852 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 678DAC5FC4C6A55F032BA40698895E6A)
- dhcpmon.exe (PID: 5400 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 678DAC5FC4C6A55F032BA40698895E6A)
  - dhcpmon.exe (PID: 160 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 678DAC5FC4C6A55F032BA40698895E6A)
- vlc.exe (PID: 5452 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: 678DAC5FC4C6A55F032BA40698895E6A)
  - vlc.exe (PID: 5372 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 678DAC5FC4C6A55F032BA40698895E6A)
  - vlc.exe (PID: 4608 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 678DAC5FC4C6A55F032BA40698895E6A)
  - vlc.exe (PID: 5504 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 678DAC5FC4C6A55F032BA40698895E6A)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "C2: ": [
    "192.253.246.143"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.503442385.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000B.00000002.503442385.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000B.00000002.503442385.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
0000000B.00000002.508585583.0000000002A81000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000027.00000002.487906789.0000000002D01000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 89 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.2AyWKsCvVF.exe.5280000.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
11.2.2AyWKsCvVF.exe.5280000.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
29.2.2AyWKsCvVF.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
29.2.2AyWKsCvVF.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
29.2.2AyWKsCvVF.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 27 entries

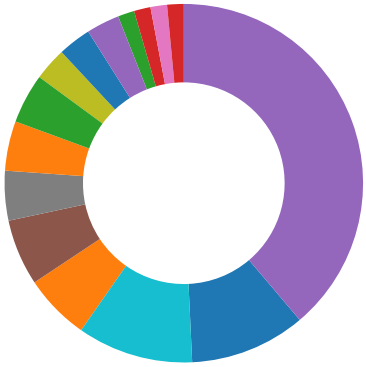
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for 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:

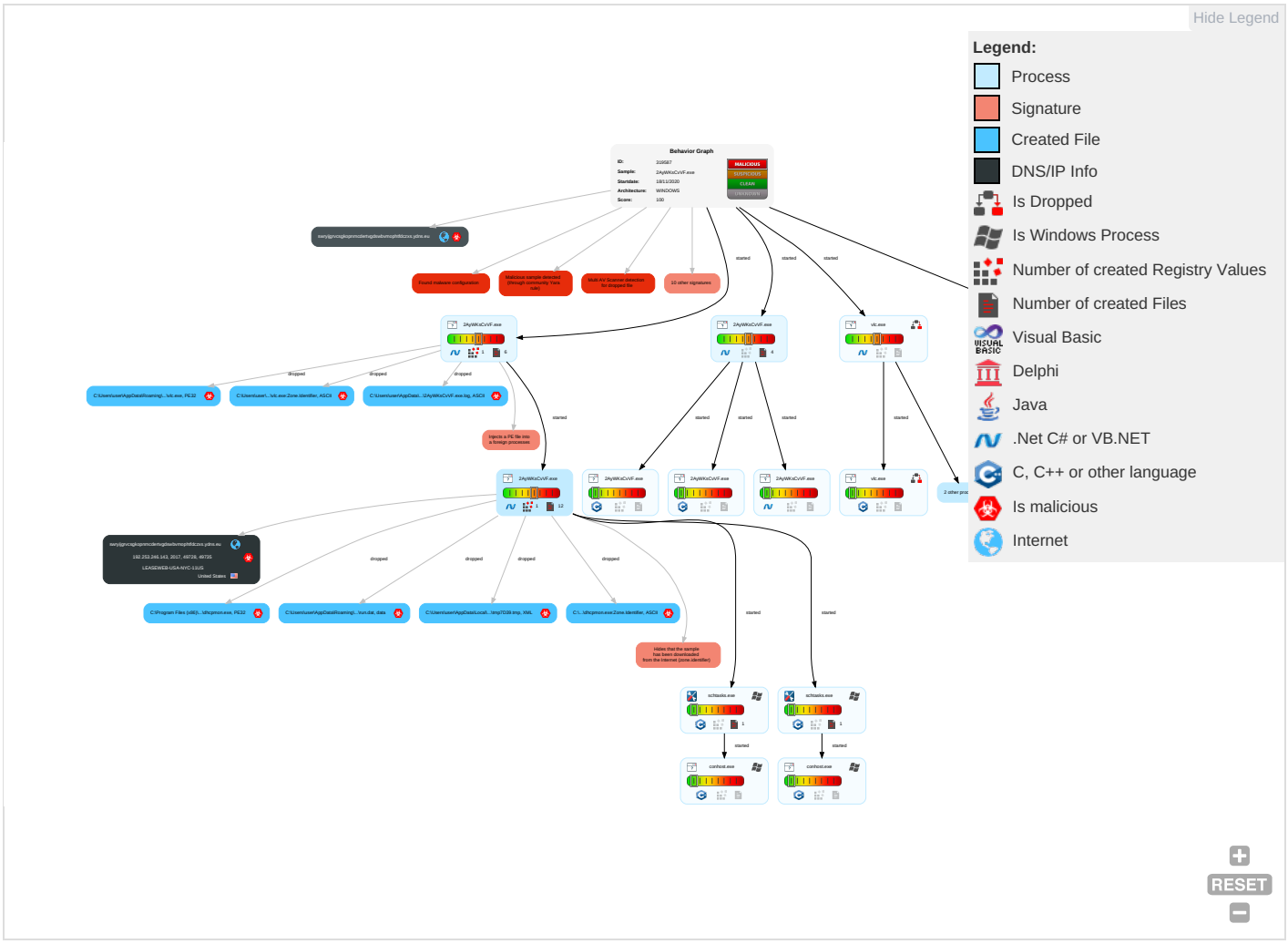
Detected Nanocore Rat

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

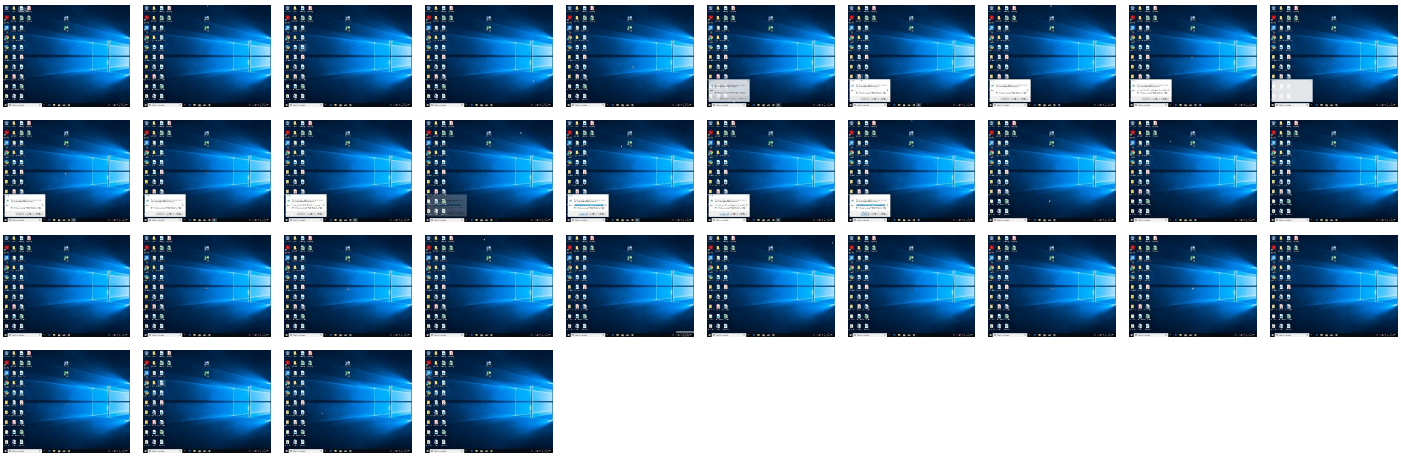
Behavior Graph



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
2AyWKsCvVF.exe	26%	Virustotal		Browse
2AyWKsCvVF.exe	23%	ReversingLabs	ByteCode-MSIL.Trojan.DelShad	
2AyWKsCvVF.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	26%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	23%	ReversingLabs	ByteCode-MSIL.Trojan.DelShad	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	23%	ReversingLabs	ByteCode-MSIL.Trojan.DelShad	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
29.2.2AyWKsCvVF.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
39.2.vlc.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.2AyWKsCvVF.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

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

Domains

Source	Detection	Scanner	Label	Link
swryijgrvcsgkopnmcdertvgdswbvmophtfdczxs.ydns.eu	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comicta	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTFB	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.coma%	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
swryijgrvcsgkopnmcdertvgdswbvmophtfdczxs.ydns.eu	192.253.246.143	true	true	• 4%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comicta	2AyWKsCvVF.exe, 00000000.00000002.321022810.0000000000EE7000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false		high

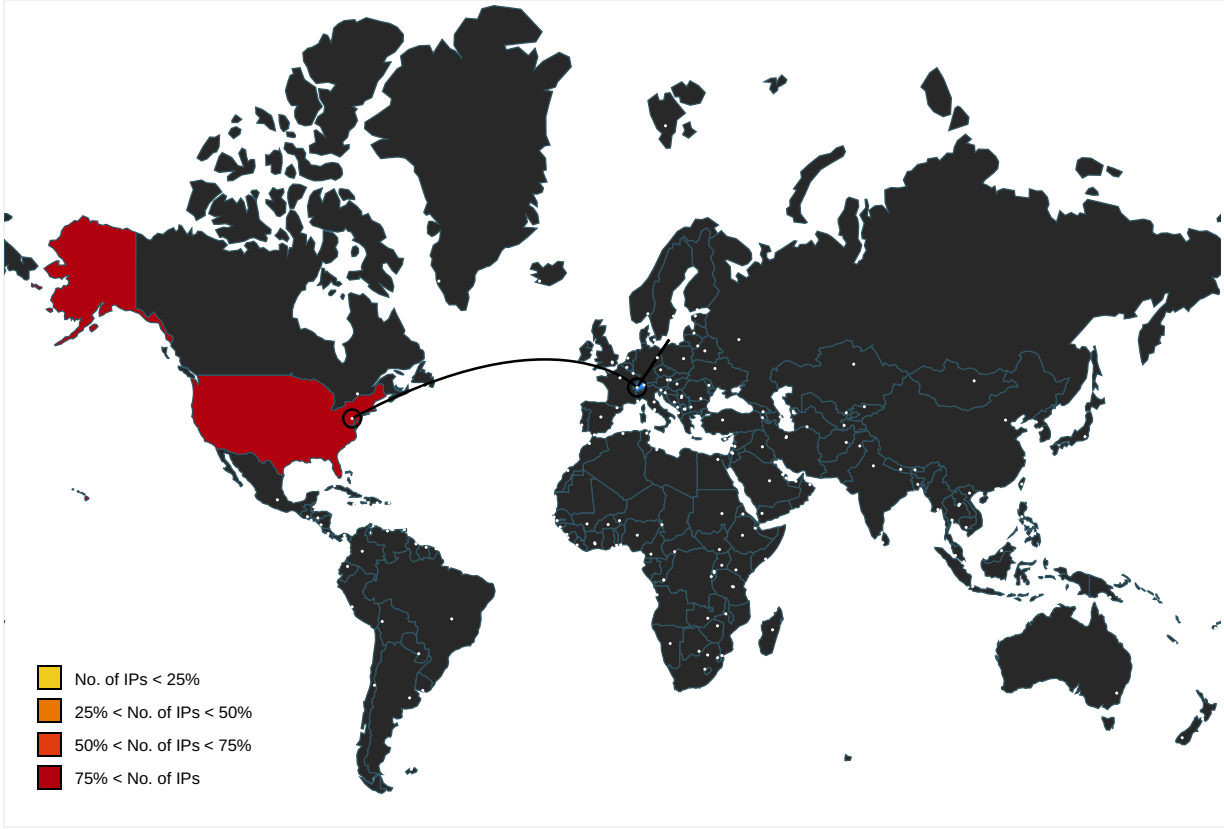
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.goodfont.co.kr	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comB.TTFB	2AyWKsCvVF.exe, 00000000.00000002.321022810.0000000000EE7000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coma	2AyWKsCvVF.exe, 00000000.00000002.321022810.0000000000EE7000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false		high
http://www.fonts.com	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	2AyWKsCvVF.exe, 00000000.00000002.334338499.00000000058F0000.00000002.00000001.sdmp, 2AyWKsCvVF.exe, 00000012.00000002.426541811.0000000006060000.00000002.00000001.sdmp, dhcpmon.exe, 00000014.00000002.440473204.0000000005570000.00000002.00000001.sdmp, vlc.exe, 00000015.00000002.447119366.0000000005500000.00000002.00000001.sdmp, dhcpmon.exe, 00000018.00000002.467839168.0000000005B80000.00000002.00000001.sdmp, vlc.exe, 0000001A.00000002.480161069.0000000005580000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma%	2AyWKsCvVF.exe, 00000000.00000002.321022810.0000000000EE7000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.253.246.143	unknown	United States		396362	LEASEWEB-USA-NYC-11US	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	319587
Start date:	18.11.2020
Start time:	13:13:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2AyWKsCvVF.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:	40
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@32/11@14/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0.6% (good quality ratio 0.5%) • Quality average: 61.3% • Quality standard deviation: 31%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.122.171.231, 104.43.193.48, 23.210.248.85, 51.104.139.180, 8.253.204.249, 67.27.235.126, 67.27.233.126, 67.26.137.254, 67.26.75.254, 40.64.100.89, 51.103.5.159, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247, 51.104.144.132 • Excluded domains from analysis (whitelisted): mw1eap.displaycatalog.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.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, 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, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, displaycatalog-uswesteap.md.mp.microsoft.com.akadns.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcolcus07.cloudapp.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
13:15:00	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run vlc "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"
13:15:02	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\2AyWKsCvVF.exe" s>$(Arg0)
13:15:02	API Interceptor	675x Sleep call for process: 2AyWKsCvVF.exe modified
13:15:05	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
13:15:08	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
13:15:17	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
192.253.246.143	HLiw2LPA8i.rtf	Get hash	malicious	Browse	
	f3wo2FuLN6.exe	Get hash	malicious	Browse	
	TLpMnhJmg7.exe	Get hash	malicious	Browse	
	HDyADDoI3I.exe	Get hash	malicious	Browse	
	3NWyBfF98R.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
swryijgrvcsgkopnmcdertvgdswbvmophtfdczxs.ydns.eu	HLiw2LPA8i.rtf	Get hash	malicious	Browse	• 192.253.246.143
	f3wo2FuLN6.exe	Get hash	malicious	Browse	• 192.253.246.143
	SecuriteInfo.com.Trojan.DownLoader35.34609.25775.exe	Get hash	malicious	Browse	• 192.253.246.138
	Payment_Order_20201111.xlsx	Get hash	malicious	Browse	• 192.253.246.138
	TLpMnhJmg7.exe	Get hash	malicious	Browse	• 192.253.246.143
	HDyADDoI3I.exe	Get hash	malicious	Browse	• 192.253.246.143
	S21Ji2TNug.exe	Get hash	malicious	Browse	• 192.253.246.141
	3NWyBfF98R.exe	Get hash	malicious	Browse	• 192.253.246.143
	22OR3ghklx.exe	Get hash	malicious	Browse	• 194.5.98.68
	2iVTzj8Bbe.exe	Get hash	malicious	Browse	• 5.135.233.28

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-USA-NYC-11US	tn9jVPvlMSqAUX5.exe	Get hash	malicious	Browse	• 23.105.131.229
	HLiw2LPA8i.rtf	Get hash	malicious	Browse	• 192.253.246.143
	TDToxqrclL.exe	Get hash	malicious	Browse	• 23.105.131.177
	Ziiq5tl3CT.exe	Get hash	malicious	Browse	• 23.105.131.239
	f3wo2FuLN6.exe	Get hash	malicious	Browse	• 192.253.246.143
	ORDER INQUIRY.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	Purchase Order 4500033557.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	SecuriteInfo.com.Trojan.DownLoader35.34609.25775.exe	Get hash	malicious	Browse	• 192.253.246.138
	Proof_of_payment.xlsm	Get hash	malicious	Browse	• 23.105.131.217
	invoice tax.xlsm	Get hash	malicious	Browse	• 23.105.131.217
	SHIPPING DOCUMENTS.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	Payment_Order_20201111.xlsx	Get hash	malicious	Browse	• 192.253.246.138
	TLpMnhJmg7.exe	Get hash	malicious	Browse	• 192.253.246.143
	HDyADDoI3I.exe	Get hash	malicious	Browse	• 192.253.246.143
	11.exe	Get hash	malicious	Browse	• 173.234.155.145
	53C29QAJnd.exe	Get hash	malicious	Browse	• 173.234.155.145
	OMQZvmAmCj.exe	Get hash	malicious	Browse	• 173.234.155.145
	gH4o5FCHAE.exe	Get hash	malicious	Browse	• 173.234.155.145
	SHIPPING INVOICE.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	DOCUMENTO WAYBILL.exe	Get hash	malicious	Browse	• 23.105.131.133

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	HLiw2LPA8i.rtf	Get hash	malicious	Browse	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	HLiw2LPA8i.rtf	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Users\user\Desktop\2AyWKsCvVF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	798720
Entropy (8bit):	7.062174295870852
Encrypted:	false
SSDEEP:	24576:Jsa5TcLNpo2AbAtY7/6RQeWXKaRXKzklCbX:baha2EAt46wXKaRDCb
MD5:	678DAC5FC4C6A55F032BA40698895E6A
SHA1:	8EA9541292F8E5D68948031EBCEDAFE04DDA4A36
SHA-256:	78491E950A624399F497CEDD25CAE2231223B1BCD2F93379480B3C9EDB4C6A92
SHA-512:	3183B4FF5E16E81BD6E0509FA473F42AE8DB8D9C9B41405E8A723BA4647DDBD58356A324B3C6FBC9AC390BC592086C07424D65ECF34EA79BD6862D7FD80C586
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 23%
Joe Sandbox View:	• Filename: HLiw2LPA8i.rtf, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....z.....v.... .....@.. ....@.....J.....v.....`..... ..... ..H.....text...|.... ..... ..`.rsrc....v.....x.....@..@.reloc.....` .....@..B.....\.....H.....F.....\.....N+.+.*(....+.(....+.6.(.....(x...*..>+.+.*.+.(....+..0..I.....-.+',.+&{....,.+ {....+..,..,.+.+..,.&&.-.* .+..+..+.o....+..+..+.(....+.....(....*..(.

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

Process:	C:\Users\user\Desktop\2AyWKsCvVF.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**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\2AyWKsCvVF.exe.log

Process:	C:\Users\user\Desktop\2AyWKsCvVF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\2AyWKsCvVF.exe.log	
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D8
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D8
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D8
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp7D39.tmp	
Process:	C:\Users\user\Desktop\2AyWKsCvVF.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1304
Entropy (8bit):	5.1124711257645075
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Jxtn:cbk4oL600QydbQxIYODOLedq3Oj
MD5:	9999914B14FFDFDDA9685849889917DE
SHA1:	67C27D3B5295EA8F29E5BA4CB10D4A6155976967
SHA-256:	56CA0B8BC6EC1B4452ABB85E020266B489D1BBB6443FA6EDEA01E335A63398E6
SHA-512:	45F3D0DB65D89F26275B1664BA00BE0406F5183C3B557EB4E533D94055D194AEC1691998E63E8F51F49E44FC97359FF214FD9D4853A505EA8DB19D248A06C051
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\tmp7D39.tmp	
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\tmp8057.tmp	
Process:	C:\Users\user\Desktop\2AyWKsCvVF.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\2AyWKsCvVF.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:lan:Un
MD5:	AC85C44515BB2C0D226060A0D1496650
SHA1:	E3730269DA672F64F46FA96F84CEDBA350523688
SHA-256:	1D6702B959BA0461DAABD1D3F87FA0F54B50F863456ECFBDB711B72C6A2CF646
SHA-512:	95D43C22198DC84EC66945636D2A39D386D69DB4CF112004688F925F4C9C1FE10AC5B779DB140C5CCCC73C3B40A4CA3DF9AF3E3C8E6AD085EF0BD4B44B2580
Malicious:	**true**
Preview:	.Lp....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\2AyWKsCvVF.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.352203688791898
Encrypted:	false
SSDEEP:	3:oN0naRRXV06jL4A:oNcSRl024A
MD5:	95361324BE4FA332D8223A825C139D50
SHA1:	72D22B0B1779C9C26ACA149661D421C3B3604657
SHA-256:	8514212D281B67AE2477555835D83674411129248B8F45FA9BD871B9B72C6A54
SHA-512:	AD6AE5DC2AC2CD53D5F797EECAFA5AF7D10F8844022700C3E60943A65BA823D013CCF4DA3CC830C374A75C708D89AEB14E9A50ED83BE53C318A6A0D00EE460E3
Malicious:	false
Preview:	C:\Users\user\Desktop\2AyWKsCvVF.exe

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	
Process:	C:\Users\user\Desktop\2AyWKsCvVF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	
Size (bytes):	798720
Entropy (8bit):	7.062174295870852
Encrypted:	false
SSDEEP:	24576:Jsa5TcLNpo2AbAtY7/6RQeWXKaRXKzklCbX:baha2EAt46wXKaRDCb
MD5:	678DAC5FC4C6A55F032BA40698895E6A
SHA1:	8EA9541292F8E5D68948031EBCEDAFE04DDA4A36
SHA-256:	78491E950A624399F497CEDD25CAE2231223B1BCD2F93379480B3C9EDB4C6A92
SHA-512:	3183B4FF5E16E81BD6E0509FA473F42AE8DB8D9C9B41405E8A723BA4647DDBD58356A324B3C6FBC9AC390BC592086C07424D65ECF34EA79BD6862D7FD80C58 6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 23%
Joe Sandbox View:	• Filename: HLiw2LPA8i.rtf, Detection: malicious, Browse
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......_....................z......v.... ....@.. ....@.................................,...J........v..................`...................................................... ............... ..H...........text...|.... ...................... ..`.rsrc....v.......x.................@..@.reloc.......` ....@..B................\.......H............F..............\..N+.+.*(....+.(....+.6.(.....(x...*..>+.+.*.+.(....+..0..I........-.+',.+&{....,.+ {....+..,..,.+.+..,.&&.-.* .+..+..+.o....+..+..+.(....+......(....*..(.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\2AyWKsCvVF.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**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.062174295870852
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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	2AyWKsCvVF.exe
File size:	798720
MD5:	678dac5fc4c6a55f032ba40698895e6a
SHA1:	8ea9541292f8e5d68948031ebcedafe04dda4a36
SHA256:	78491e950a624399f497cedd25cae2231223b1bcd2f93379480b3c9edb4c6a92
SHA512:	3183b4ff5e16e81bd6e0509fa473f42ae8db8d9c9b41405e8a723ba4647ddbd58356a324b3c6fbc9ac390bc592086c07424d65ecf34ea79bd6862d7fd80c58c6
SSDEEP:	24576:Jsa5TcLNpo2AbAtY7/6RQeWXKaRXKzklCbX:baha2EAt46wXKaRDCb
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......_.....................z......v.... ....@.. ....@................................

File Icon

Icon Hash:	74f2dbb284c2e2ee

Static PE Info

General

Entrypoint:	0x47d376
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FB48592 [Wed Nov 18 02:23:14 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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
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	0x7d32c	0x4a	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7e000	0x47615	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc6000	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	0x7b37c	0x7b400	False	0.946120689655	data	7.93617451115	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7e000	0x47615	0x47800	False	0.200171410621	data	4.66082809621	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc6000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x7e08c	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	0xc00d8	0x25a8	data		
RT_ICON	0xc26a4	0x10a8	data		
RT_ICON	0xc3770	0x988	data		
RT_ICON	0xc411c	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xc45c0	0x4c	data		
RT_VERSION	0xc4648	0x33c	data		
RT_MANIFEST	0xc49c0	0xc55	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF 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	ABW.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	ABW.exe

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 13:15:04.257178068 CET	49728	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:04.567527056 CET	2017	49728	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:05.163006067 CET	49728	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:05.473237038 CET	2017	49728	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:05.980878115 CET	49728	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:06.291510105 CET	2017	49728	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:10.527563095 CET	49735	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:10.866230011 CET	2017	49735	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:11.418787003 CET	49735	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:11.838531971 CET	2017	49735	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:12.418890953 CET	49735	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:12.750057936 CET	2017	49735	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:16.804665089 CET	49746	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:17.159245014 CET	2017	49746	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:17.719794989 CET	49746	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:18.078959942 CET	2017	49746	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:18.591330051 CET	49746	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:18.999630928 CET	2017	49746	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:23.247824907 CET	49747	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:23.603555918 CET	2017	49747	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:24.107378960 CET	49747	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:24.423556089 CET	2017	49747	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:25.107481956 CET	49747	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:25.447871923 CET	2017	49747	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:29.492758036 CET	49748	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:29.854454041 CET	2017	49748	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:30.467434883 CET	49748	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:36.467822075 CET	49748	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:36.779057026 CET	2017	49748	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:41.064198017 CET	49749	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:41.429009914 CET	2017	49749	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:41.937490940 CET	49749	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:42.348604918 CET	2017	49749	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:42.858931065 CET	49749	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:43.269334078 CET	2017	49749	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:47.367022991 CET	49750	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:47.674303055 CET	2017	49750	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:48.187544107 CET	49750	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:48.593672037 CET	2017	49750	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:49.094141006 CET	49750	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:49.409420967 CET	2017	49750	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:53.465146065 CET	49753	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:53.816565037 CET	2017	49753	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:54.328711033 CET	49753	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:54.742865086 CET	2017	49753	192.253.246.143	192.168.2.7
Nov 18, 2020 13:15:55.250633001 CET	49753	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:15:55.561321020 CET	2017	49753	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:00.023139000 CET	49754	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:00.333301067 CET	2017	49754	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:00.845179081 CET	49754	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:01.188616037 CET	2017	49754	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:01.704370022 CET	49754	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:02.110388994 CET	2017	49754	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:06.181993008 CET	49755	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:06.489480019 CET	2017	49755	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:07.001641989 CET	49755	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:07.330274105 CET	2017	49755	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:07.845446110 CET	49755	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:08.251686096 CET	2017	49755	192.253.246.143	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 13:16:12.310183048 CET	49756	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:12.659724951 CET	2017	49756	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:13.174256086 CET	49756	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:13.485918045 CET	2017	49756	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:13.986845016 CET	49756	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:14.344104052 CET	2017	49756	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:18.510282993 CET	49757	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:18.820801973 CET	2017	49757	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:19.330920935 CET	49757	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:19.722898006 CET	2017	49757	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:20.238782883 CET	49757	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:20.644606113 CET	2017	49757	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:24.696957111 CET	49758	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:25.049243927 CET	2017	49758	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:25.565699100 CET	49758	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:25.877461910 CET	2017	49758	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:26.379347086 CET	49758	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:26.691189051 CET	2017	49758	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:30.743957043 CET	49759	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:31.091018915 CET	2017	49759	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:31.597387075 CET	49759	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:31.936604977 CET	2017	49759	192.253.246.143	192.168.2.7
Nov 18, 2020 13:16:32.441303968 CET	49759	2017	192.168.2.7	192.253.246.143
Nov 18, 2020 13:16:32.752310038 CET	2017	49759	192.253.246.143	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 13:14:16.334083080 CET	60338	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:16.361186028 CET	53	60338	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:17.258542061 CET	58717	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:17.294179916 CET	53	58717	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:18.220112085 CET	59762	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:18.247369051 CET	53	59762	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:19.088411093 CET	54329	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:19.115885019 CET	53	54329	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:20.013658047 CET	58052	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:20.040905952 CET	53	58052	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:20.973460913 CET	54008	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:21.000807047 CET	53	54008	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:21.994016886 CET	59451	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:22.030141115 CET	53	59451	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:22.903172970 CET	52914	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:22.940905094 CET	53	52914	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:23.796224117 CET	64569	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:23.823364973 CET	53	64569	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:24.710278034 CET	52816	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:24.737350941 CET	53	52816	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:25.549248934 CET	50781	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:25.576479912 CET	53	50781	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:26.507963896 CET	54230	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:26.535109997 CET	53	54230	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:27.400171041 CET	54911	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:27.427227974 CET	53	54911	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:28.241380930 CET	49958	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:28.268456936 CET	53	49958	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:29.083427906 CET	50860	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:29.110635996 CET	53	50860	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:30.338119984 CET	50452	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:30.368040085 CET	53	50452	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:31.185043097 CET	59730	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:31.212316036 CET	53	59730	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:32.050189018 CET	59310	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:32.085835934 CET	53	59310	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 13:14:32.627278090 CET	51919	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:32.664104939 CET	53	51919	8.8.8.8	192.168.2.7
Nov 18, 2020 13:14:42.595653057 CET	64296	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:14:42.622812986 CET	53	64296	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:02.741520882 CET	56680	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:02.768811941 CET	53	56680	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:04.144943953 CET	58820	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:04.172987938 CET	60983	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:04.203042030 CET	53	58820	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:04.208764076 CET	53	60983	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:04.411902905 CET	49247	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:04.462351084 CET	53	49247	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:05.393771887 CET	52286	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:05.429589033 CET	53	52286	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:05.994560957 CET	56064	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:06.030332088 CET	53	56064	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:07.482305050 CET	63744	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:07.517927885 CET	53	63744	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:09.852799892 CET	61457	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:09.888607979 CET	53	61457	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:10.418124914 CET	58367	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:10.454072952 CET	53	58367	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:10.487066984 CET	60599	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:10.522847891 CET	53	60599	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:10.974488974 CET	59571	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:11.001782894 CET	53	59571	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:11.025796890 CET	52689	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:11.052932978 CET	53	52689	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:12.653100967 CET	50290	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:12.688760042 CET	53	50290	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:14.375849009 CET	60427	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:14.411693096 CET	53	60427	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:15.742705107 CET	56209	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:15.780607939 CET	53	56209	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:16.661848068 CET	59582	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:16.698621035 CET	53	59582	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:16.767863035 CET	60949	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:16.803494930 CET	53	60949	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:23.192267895 CET	58542	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:23.243531942 CET	53	58542	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:29.455739975 CET	59179	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:29.491556883 CET	53	59179	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:40.852751017 CET	60927	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:40.888389111 CET	53	60927	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:47.328639984 CET	57854	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:47.364285946 CET	53	57854	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:48.831229925 CET	62026	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:48.858542919 CET	53	62026	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:52.543030024 CET	59453	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:52.570125103 CET	53	59453	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:53.427609921 CET	62468	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:15:53.463145018 CET	53	62468	8.8.8.8	192.168.2.7
Nov 18, 2020 13:15:59.986233950 CET	52563	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:16:00.021874905 CET	53	52563	8.8.8.8	192.168.2.7
Nov 18, 2020 13:16:06.144609928 CET	54721	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:16:06.180191040 CET	53	54721	8.8.8.8	192.168.2.7
Nov 18, 2020 13:16:12.271882057 CET	62826	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:16:12.307739019 CET	53	62826	8.8.8.8	192.168.2.7
Nov 18, 2020 13:16:18.472783089 CET	62046	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:16:18.508119106 CET	53	62046	8.8.8.8	192.168.2.7
Nov 18, 2020 13:16:24.660619974 CET	51223	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:16:24.696073055 CET	53	51223	8.8.8.8	192.168.2.7
Nov 18, 2020 13:16:30.707820892 CET	63908	53	192.168.2.7	8.8.8.8
Nov 18, 2020 13:16:30.743345022 CET	53	63908	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 18, 2020 13:15:04.144943953 CET	192.168.2.7	8.8.8.8	0xd869	Standard query (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu	A (IP address)	IN (0x0001)
Nov 18, 2020 13:15:10.487066984 CET	192.168.2.7	8.8.8.8	0xa36c	Standard query (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu	A (IP address)	IN (0x0001)
Nov 18, 2020 13:15:16.767863035 CET	192.168.2.7	8.8.8.8	0xe976	Standard query (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu	A (IP address)	IN (0x0001)
Nov 18, 2020 13:15:23.192267895 CET	192.168.2.7	8.8.8.8	0x138	Standard query (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu	A (IP address)	IN (0x0001)
Nov 18, 2020 13:15:29.455739975 CET	192.168.2.7	8.8.8.8	0x29e3	Standard query (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu	A (IP address)	IN (0x0001)
Nov 18, 2020 13:15:40.852751017 CET	192.168.2.7	8.8.8.8	0x5b7d	Standard query (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu	A (IP address)	IN (0x0001)
Nov 18, 2020 13:15:47.328639984 CET	192.168.2.7	8.8.8.8	0xd630	Standard query (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu	A (IP address)	IN (0x0001)
Nov 18, 2020 13:15:53.427609921 CET	192.168.2.7	8.8.8.8	0xaa4c	Standard query (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu	A (IP address)	IN (0x0001)
Nov 18, 2020 13:15:59.986233950 CET	192.168.2.7	8.8.8.8	0x76be	Standard query (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu	A (IP address)	IN (0x0001)
Nov 18, 2020 13:16:06.144609928 CET	192.168.2.7	8.8.8.8	0x6be6	Standard query (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu	A (IP address)	IN (0x0001)
Nov 18, 2020 13:16:12.271882057 CET	192.168.2.7	8.8.8.8	0x6a7a	Standard query (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu	A (IP address)	IN (0x0001)
Nov 18, 2020 13:16:18.472783089 CET	192.168.2.7	8.8.8.8	0xfb93	Standard query (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu	A (IP address)	IN (0x0001)
Nov 18, 2020 13:16:24.660619974 CET	192.168.2.7	8.8.8.8	0x6c99	Standard query (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu	A (IP address)	IN (0x0001)
Nov 18, 2020 13:16:30.707820892 CET	192.168.2.7	8.8.8.8	0x98a6	Standard query (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu	A (IP address)	IN (0x0001)

DNS Answers

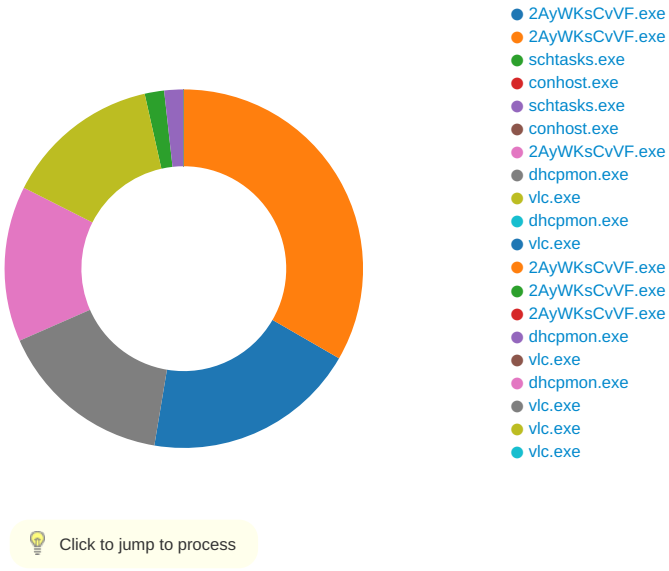
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 18, 2020 13:15:04.203042030 CET	8.8.8.8	192.168.2.7	0xd869	No error (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu		192.253.246.143	A (IP address)	IN (0x0001)
Nov 18, 2020 13:15:10.522847891 CET	8.8.8.8	192.168.2.7	0xa36c	No error (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu		192.253.246.143	A (IP address)	IN (0x0001)
Nov 18, 2020 13:15:16.803494930 CET	8.8.8.8	192.168.2.7	0xe976	No error (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu		192.253.246.143	A (IP address)	IN (0x0001)
Nov 18, 2020 13:15:23.243531942 CET	8.8.8.8	192.168.2.7	0x138	No error (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu		192.253.246.143	A (IP address)	IN (0x0001)
Nov 18, 2020 13:15:29.491556883 CET	8.8.8.8	192.168.2.7	0x29e3	No error (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu		192.253.246.143	A (IP address)	IN (0x0001)
Nov 18, 2020 13:15:40.888389111 CET	8.8.8.8	192.168.2.7	0x5b7d	No error (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu		192.253.246.143	A (IP address)	IN (0x0001)
Nov 18, 2020 13:15:47.364285946 CET	8.8.8.8	192.168.2.7	0xd630	No error (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu		192.253.246.143	A (IP address)	IN (0x0001)
Nov 18, 2020 13:15:53.463145018 CET	8.8.8.8	192.168.2.7	0xaa4c	No error (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu		192.253.246.143	A (IP address)	IN (0x0001)
Nov 18, 2020 13:16:00.021874905 CET	8.8.8.8	192.168.2.7	0x76be	No error (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu		192.253.246.143	A (IP address)	IN (0x0001)
Nov 18, 2020 13:16:06.180191040 CET	8.8.8.8	192.168.2.7	0x6be6	No error (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu		192.253.246.143	A (IP address)	IN (0x0001)
Nov 18, 2020 13:16:12.307739019 CET	8.8.8.8	192.168.2.7	0x6a7a	No error (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu		192.253.246.143	A (IP address)	IN (0x0001)
Nov 18, 2020 13:16:18.508119106 CET	8.8.8.8	192.168.2.7	0xfb93	No error (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu		192.253.246.143	A (IP address)	IN (0x0001)
Nov 18, 2020 13:16:24.696073055 CET	8.8.8.8	192.168.2.7	0x6c99	No error (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu		192.253.246.143	A (IP address)	IN (0x0001)
Nov 18, 2020 13:16:30.743345022 CET	8.8.8.8	192.168.2.7	0x98a6	No error (0)	swryijgrvc sgkopnmcde rtvgdswbvm ophtfdczxs .ydns.eu		192.253.246.143	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 2AyWKsCvVF.exe PID: 6776 Parent PID: 5668

General

Start time:	13:14:19
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\2AyWKsCvVF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\2AyWKsCvVF.exe'
Imagebase:	0x4b0000
File size:	798720 bytes
MD5 hash:	678DAC5FC4C6A55F032BA40698895E6A
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: 00000000.00000002.324205018.00000000037D9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.324205018.00000000037D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.324205018.00000000037D9000.00000004.00000001.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	6D4ACF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D4ACF06	unknown
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	6C2FBEFF	CreateDirectoryW
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	75FCC73	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	75FCC73	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\2AyWKsCvVF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D7BC78D	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 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 92 85 b4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 b4 07 00 00 7a 04 00 00 00 00 00 76 d3 07 00 00 20 00 00 00 e0 07 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 0c 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......_.......... ....z......v.... ....@.. ....@.................	success or wait	4	75FCC73	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	75FCC73	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\2AyWKsCvVF.exe.log	unknown	1119	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 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D7BC907	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	6D485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D485705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D48CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C2F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C2F1B4F	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	6C2F646A	RegSetValueExW

Analysis Process: 2AyWKsCvVF.exe PID: 6448 Parent PID: 6776

General

Start time:	13:14:57
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\2AyWKsCvVF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\2AyWKsCvVF.exe
Imagebase:	0x690000
File size:	798720 bytes
MD5 hash:	678DAC5FC4C6A55F032BA40698895E6A
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: 0000000B.00000002.503442385.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.503442385.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.503442385.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.508585583.0000000002A81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.512799429.0000000003A89000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.512799429.0000000003A89000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.515934182.0000000006070000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.515934182.0000000006070000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.515934182.0000000006070000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.515202171.0000000005280000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.515202171.0000000005280000.00000004.00000001.sdmp, Author: Florian Roth
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	6D4ACF06	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	6D4ACF06	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	6C2FBEFF	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	6C2F1E60	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	6C2FBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6C2FDD66	CopyFileW
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	6C2FDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7D39.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C2F7038	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	6C2F1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp8057.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C2F7038	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	6C2FBEFF	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	6C2FBEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7D39.tmp	success or wait	1	6C2F6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp8057.tmp	success or wait	1	6C2F6A95	DeleteFileW
C:\Users\user\Desktop\2AyWKsCvVF.exe:Zone.Identifier	success or wait	1	6C272935	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	04 4c 70 02 07 8c d8 48	.Lp....H	success or wait	1	6C2F1B4F	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 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 92 85 b4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 b4 07 00 00 7a 04 00 00 00 00 00 76 d3 07 00 00 20 00 00 00 e0 07 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 0c 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......_.......... ....z......v.... ....@.. ....@................	success or wait	4	6C2FDD66	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	6C2FDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7D39.tmp	unknown	1304	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	6C2F1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	41	43 3a 5c 55 73 65 72 73 5c 66 72 6f 6e 74 64 65 73 6b 5c 44 65 73 6b 74 6f 70 5c 32 41 79 57 4b 73 43 76 56 46 2e 65 78 65	C:\Users\user\Desktop\2A yWKsCvVF.exe	success or wait	1	6C2F1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8057.tmp	unknown	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	6C2F1B4F	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	6D485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D485705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D48CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C2F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C2F1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D46D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D46D72F	unknown
C:\Users\user\Desktop\2AyWKsCvVF.exe	unknown	4096	success or wait	1	6D46D72F	unknown
C:\Users\user\Desktop\2AyWKsCvVF.exe	unknown	512	success or wait	1	6D46D72F	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	6C2F646A	RegSetValueExW

Analysis Process: schtasks.exe PID: 6924 Parent PID: 6448

General

Start time:	13:15:00
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\tmp7D39.tmp'
Imagebase:	0x13b0000
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\tmp7D39.tmp	unknown	2	success or wait	1	13BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7D39.tmp	unknown	1305	success or wait	1	13BABD9	ReadFile

Analysis Process: conhost.exe PID: 6940 Parent PID: 6924

General

Start time:	13:15:01
Start date:	18/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 7116 Parent PID: 6448

General

Start time:	13:15:01
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\tmp8057.tmp'
Imagebase:	0x13b0000
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\tmp8057.tmp	unknown	2	success or wait	1	13BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8057.tmp	unknown	1311	success or wait	1	13BABD9	ReadFile

Analysis Process: conhost.exe PID: 7124 Parent PID: 7116

General

Start time:	13:15:02
Start date:	18/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 2AyWKsCvVF.exe PID: 5644 Parent PID: 1104

General

Start time:	13:15:02
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\2AyWKsCvVF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\2AyWKsCvVF.exe 0
Imagebase:	0xcd0000
File size:	798720 bytes
MD5 hash:	678DAC5FC4C6A55F032BA40698895E6A
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: 00000012.00000002.413173829.00000000040F9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.413173829.00000000040F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.413173829.00000000040F9000.00000004.00000001.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	6D4ACF06	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	6D4ACF06	unknown
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	793CC73	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	793CC73	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	6D485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D485705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D48CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C2F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C2F1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: 6976 Parent PID: 1104

General

Start time:	13:15:05
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:	0x1c0000
File size:	798720 bytes
MD5 hash:	678DAC5FC4C6A55F032BA40698895E6A
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: 00000014.00000002.428448474.0000000003569000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.428448474.0000000003569000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.428448474.0000000003569000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 26%, Virustotal, Browse • Detection: 23%, ReversingLabs
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	6D4ACF06	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	6D4ACF06	unknown
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	6F6CC73	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	6F6CC73	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	6D7BC78D	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	1119	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 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D7BC907	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	6D485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D485705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D48CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C2F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C2F1B4F	ReadFile

Analysis Process: vlc.exe PID: 5720 Parent PID: 3292

General

Start time:	13:15:08
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:	0x80000
File size:	798720 bytes
MD5 hash:	678DAC5FC4C6A55F032BA40698895E6A
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: 00000015.00000002.433776736.0000000003479000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.433776736.0000000003479000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.433776736.0000000003479000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 23%, ReversingLabs
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	6D4ACF06	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	6D4ACF06	unknown
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	6D7BC78D	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	1119	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 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D7BC907	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	6D485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D485705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D48CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C2F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C2F1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: 5400 Parent PID: 3292

General

Start time:	13:15:18
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:	0x600000
File size:	798720 bytes
MD5 hash:	678DAC5FC4C6A55F032BA40698895E6A
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: 00000018.00000002.462834222.0000000003C59000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.462834222.0000000003C59000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.462834222.0000000003C59000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: vlc.exe PID: 5452 Parent PID: 3292

General

Start time:	13:15:26
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:	0x230000
File size:	798720 bytes
MD5 hash:	678DAC5FC4C6A55F032BA40698895E6A
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: 0000001A.00000002.473151225.00000000035A9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000002.473151225.00000000035A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000002.473151225.00000000035A9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: 2AyWKsCvVF.exe PID: 5576 Parent PID: 5644

General

Start time:	13:15:36
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\2AyWKsCvVF.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\2AyWKsCvVF.exe
Imagebase:	0x10000
File size:	798720 bytes
MD5 hash:	678DAC5FC4C6A55F032BA40698895E6A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 2AyWKsCvVF.exe PID: 5716 Parent PID: 5644

General

Start time:	13:15:37
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\2AyWKsCvVF.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\2AyWKsCvVF.exe
Imagebase:	0x310000
File size:	798720 bytes
MD5 hash:	678DAC5FC4C6A55F032BA40698895E6A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 2AyWKsCvVF.exe PID: 4164 Parent PID: 5644

General

Start time:	13:15:37
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\2AyWKsCvVF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\2AyWKsCvVF.exe
Imagebase:	0xfc0000
File size:	798720 bytes
MD5 hash:	678DAC5FC4C6A55F032BA40698895E6A
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: 0000001D.00000002.428411812.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000002.428411812.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000002.428411812.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000002.433424124.0000000004439000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000002.433424124.0000000004439000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000002.433041265.0000000003431000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000002.433041265.0000000003431000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: dhcpmon.exe PID: 5000 Parent PID: 6976

General

Start time:	13:15:43
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:	0xb30000
File size:	798720 bytes
MD5 hash:	678DAC5FC4C6A55F032BA40698895E6A
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: 0000001F.00000002.443489424.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001F.00000002.443489424.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001F.00000002.443489424.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001F.00000002.453662342.00000000040F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001F.00000002.453662342.00000000040F9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001F.00000002.452648139.00000000030F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001F.00000002.452648139.00000000030F1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: vlc.exe PID: 852 Parent PID: 5720

General

Start time:	13:15:43
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:	0xea0000
File size:	798720 bytes

MD5 hash:	678DAC5FC4C6A55F032BA40698895E6A
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: 00000021.00000002.454007253.0000000004299000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000002.454007253.0000000004299000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000021.00000002.444761456.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000002.444761456.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000002.444761456.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000002.453327422.0000000003291000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000002.453327422.0000000003291000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: dhcpmon.exe PID: 160 Parent PID: 5400

General

Start time:	13:15:55
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:	0xa60000
File size:	798720 bytes
MD5 hash:	678DAC5FC4C6A55F032BA40698895E6A
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: 00000023.00000002.475445043.0000000002F11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000023.00000002.475445043.0000000002F11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000023.00000002.471978530.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000023.00000002.471978530.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000023.00000002.471978530.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000023.00000002.475606166.0000000003F19000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000023.00000002.475606166.0000000003F19000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: vlc.exe PID: 5372 Parent PID: 5452

General

Start time:	13:16:04
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:	0x240000
File size:	798720 bytes
MD5 hash:	678DAC5FC4C6A55F032BA40698895E6A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: vlc.exe PID: 4608 Parent PID: 5452

General

Start time:	13:16:05
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:	0x2b0000
File size:	798720 bytes
MD5 hash:	678DAC5FC4C6A55F032BA40698895E6A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: vlc.exe PID: 5504 Parent PID: 5452

General

Start time:	13:16:06
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:	0x890000
File size:	798720 bytes
MD5 hash:	678DAC5FC4C6A55F032BA40698895E6A
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: 00000027.00000002.487906789.0000000002D01000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000027.00000002.487906789.0000000002D01000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000027.00000002.486406392.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000027.00000002.486406392.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000027.00000002.486406392.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000027.00000002.488034927.0000000003D09000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000027.00000002.488034927.0000000003D09000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis