



ID: 319216
Sample Name: CDC GUIDES COVID-19 Second Outbreak Warning release.scr
Cookbook: default.jbs
Time: 05:46:57
Date: 18/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report CDC GUIDES COVID-19 Second Outbreak Warning release.scr 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Signature Overview 6
AV Detection: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 13
Public 13
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASN 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 18
General 18
File Icon 18
Static PE Info 19
General 19

Authenticode Signature 19
Entrypoint Preview 19
Data Directories 21
Sections 21
Resources 21
Imports 21
Network Behavior 22
Network Port Distribution 22
TCP Packets 22
UDP Packets 23
DNS Queries 25
DNS Answers 25
HTTP Request Dependency Graph 25
HTTP Packets 25
Code Manipulations 26
Statistics 26
Behavior 26
System Behavior 26
Analysis Process: CDC GUIDES COVID-19 Second Outbreak Warning release.exe PID: 2764 Parent PID: 566426
General 26
File Activities 26
File Created 26
File Written 27
File Read 28
Registry Activities 28
Key Value Created 28
Analysis Process: CDC GUIDES COVID-19 Second Outbreak Warning release.exe PID: 5820 Parent PID: 276428
General 28
File Activities 29
File Created 29
File Written 29
File Read 30
Registry Activities 30
Analysis Process: vlc.exe PID: 6588 Parent PID: 3388 30
General 30
File Activities 31
File Created 31
File Written 31
File Read 31
Analysis Process: vlc.exe PID: 6824 Parent PID: 3388 32
General 32
File Activities 32
File Read 32
Analysis Process: vlc.exe PID: 2172 Parent PID: 6588 32
General 32
File Activities 33
File Created 33
File Read 33
Analysis Process: vlc.exe PID: 4080 Parent PID: 6824 33
General 33
File Activities 33
File Created 33
File Read 34
Analysis Process: 9FFWrx9i8Kuq.exe PID: 496 Parent PID: 5820 34
General 34
File Activities 34
File Created 34
File Read 34
Disassembly 35
Code Analysis 35

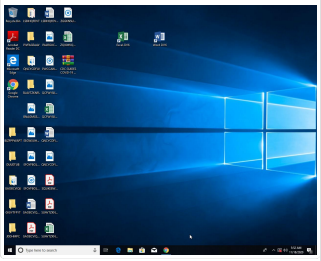
Analysis Report CDC GUIDES COVID-19 Second Outbre…

Overview

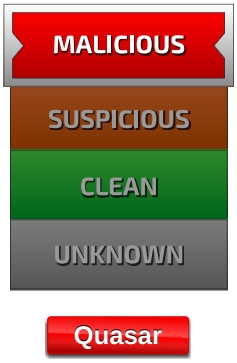
General Information

Sample Name:	CDC GUIDES COVID-19 Second Outbreak Warning release.scr (renamed file extension from scr to exe)
Analysis ID:	319216
MD5:	dc8d9c9a86fe483..
SHA1:	a63fa3cc878efe7..
SHA256:	5dcd1649d97e0d..

Most interesting Screenshot:



Detection



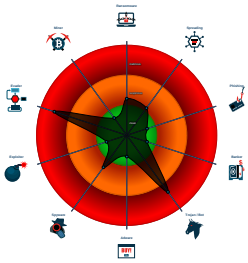
Quasar

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

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected Quasar RAT
- .NET source code references suspic…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- May check the online IP address of …
- Queries sensitive BIOS Information …
- Tries to detect sandboxes and other…
- Contains long sleeps (>= 3 min)
- Creates a DirectInput object (often fo…

Classification



Startup

- **System is w10x64**
- CDC GUIDES COVID-19 Second Outbreak Warning release.exe (PID: 2764 cmdline: 'C:\Users\user\Desktop\CDC GUIDES COVID-19 Second Outbreak Warning release.exe' MD5: DC8D9C9A86FE4830053697C1DC59DC6F)
  - CDC GUIDES COVID-19 Second Outbreak Warning release.exe (PID: 5820 cmdline: C:\Users\user\Desktop\CDC GUIDES COVID-19 Second Outbreak Warning release.exe MD5: DC8D9C9A86FE4830053697C1DC59DC6F)
    - 9FFWrx9i8Kuq.exe (PID: 496 cmdline: C:\Users\user\AppData\Local\Temp\9FFWrx9i8Kuq.exe MD5: 082B27BB1AAA169A5D0C4CD536976F99)
- vlc.exe (PID: 6588 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: DC8D9C9A86FE4830053697C1DC59DC6F)
  - vlc.exe (PID: 2172 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: DC8D9C9A86FE4830053697C1DC59DC6F)
- vlc.exe (PID: 6824 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: DC8D9C9A86FE4830053697C1DC59DC6F)
  - vlc.exe (PID: 4080 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: DC8D9C9A86FE4830053697C1DC59DC6F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Copyright null 2020

Source	Rule	Description	Author	Strings
0000000F.00000002.372345849.0000000003BE5000.00000004.00000001.sdmp	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0xe70d7:$s1: DoUploadAndExecute • 0x13def7:$s1: DoUploadAndExecute • 0xe731b:$s2: DoDownloadAndExecute • 0x13e13b:$s2: DoDownloadAndExecute • 0xe6e9c:$s3: DoShellExecute • 0x13dcbc:$s3: DoShellExecute • 0xe72d3:$s4: set_Processname • 0x13e0f3:$s4: set_Processname • 0xae9d4:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x1057f4:$op1: 04 1E FE 02 04 16 FE 01 60 • 0xae8f8:$op2: 00 17 03 1F 20 17 19 15 28 • 0x105718:$op2: 00 17 03 1F 20 17 19 15 28 • 0xaf35e:$op3: 00 04 03 69 91 1B 40 • 0xafbae:$op3: 00 04 03 69 91 1B 40 • 0x10617e:$op3: 00 04 03 69 91 1B 40 • 0x1069ce:$op3: 00 04 03 69 91 1B 40
0000000F.00000002.372345849.0000000003BE5000.00000004.00000001.sdmp	JoeSecurity_Quasar	Yara detected Quasar RAT	Joe Security	
00000005.00000002.831738365.0000000000402000.00000040.00000001.sdmp	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x3df27:$s1: DoUploadAndExecute • 0x3e16b:$s2: DoDownloadAndExecute • 0x3dcec:$s3: DoShellExecute • 0x3e123:$s4: set_Processname • 0x5824:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x5748:$op2: 00 17 03 1F 20 17 19 15 28 • 0x61ae:$op3: 00 04 03 69 91 1B 40 • 0x69fe:$op3: 00 04 03 69 91 1B 40
00000005.00000002.831738365.0000000000402000.00000040.00000001.sdmp	JoeSecurity_Quasar	Yara detected Quasar RAT	Joe Security	
00000014.00000002.358547843.0000000000402000.00000040.00000001.sdmp	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x3df27:$s1: DoUploadAndExecute • 0x3e16b:$s2: DoDownloadAndExecute • 0x3dcec:$s3: DoShellExecute • 0x3e123:$s4: set_Processname • 0x5824:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x5748:$op2: 00 17 03 1F 20 17 19 15 28 • 0x61ae:$op3: 00 04 03 69 91 1B 40 • 0x69fe:$op3: 00 04 03 69 91 1B 40

Click to see the 13 entries

Unpacked PEs

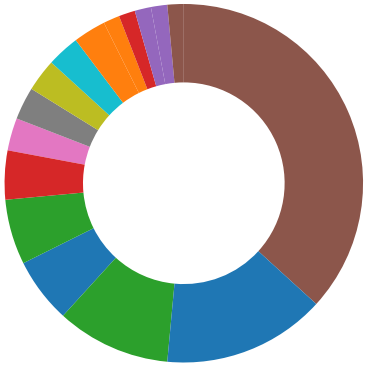
Source	Rule	Description	Author	Strings
21.2.vlc.exe.400000.0.unpack	Vermin_Keylogger_Jan18_1	Detects Vermin Keylogger	Florian Roth	• 0x3ec0a:$x3: GetKeyloggerLogsResponse • 0x3de62:$x4: GetKeyloggerLogs • 0x3e13a:$s1: <RunHidden>k__BackingField • 0x3edd2:$s2: set_SystemInfos • 0x3e163:$s3: set_RunHidden • 0x3dc96:$s4: set_RemotePath • 0x56628:$s6: Client.exe • 0x566bc:$s6: Client.exe • 0x32029:$s7: xClient.Core.ReverseProxy.Packets
21.2.vlc.exe.400000.0.unpack	xRAT_1	Detects Patchwork malware	Florian Roth	• 0x305c0:$x4: xClient.Properties.Resources.resources • 0x30481:$s4: Client.exe • 0x3e163:$s7: set_RunHidden
21.2.vlc.exe.400000.0.unpack	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x3e127:$s1: DoUploadAndExecute • 0x3e36b:$s2: DoDownloadAndExecute • 0x3deec:$s3: DoShellExecute • 0x3e323:$s4: set_Processname • 0x5a24:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x5948:$op2: 00 17 03 1F 20 17 19 15 28 • 0x63ae:$op3: 00 04 03 69 91 1B 40 • 0x6bfe:$op3: 00 04 03 69 91 1B 40
21.2.vlc.exe.400000.0.unpack	Quasar_RAT_2	Detects Quasar RAT	Florian Roth	• 0x3ec0a:$x1: GetKeyloggerLogsResponse • 0x3ee4a:$s1: DoShellExecuteResponse • 0x3e7b9:$s2: GetPasswordsResponse • 0x3ed1d:$s3: GetStartupItemsResponse • 0x3e13b:$s5: RunHidden • 0x3e159:$s5: RunHidden • 0x3e167:$s5: RunHidden • 0x3e17b:$s5: RunHidden
21.2.vlc.exe.400000.0.unpack	MAL_QuasarRAT_May19_1	Detects QuasarRAT malware	Florian Roth	• 0x4f649:$xc1: 41 00 64 00 6D 00 69 00 6E 00 00 11 73 00 63 00 68 00 74 00 61 00 73 00 6B 00 73 00 00 1B 2F 00 ... • 0x4f87f:$xc2: 00 70 00 69 00 6E 00 67 00 20 00 2D 00 6E 00 20 00 31 00 30 00 20 00 6C 00 6F 00 63 00 61 00 6C ...

Click to see the 16 entries

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Quasar RAT

Machine Learning detection for dropped file

Networking:



May check the online IP address of the machine

E-Banking Fraud:



Yara detected Quasar RAT

System Summary:



Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:



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

Malware Analysis System Evasion:



Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

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

HIPS / PFW / Operating System Protection Evasion:



.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information:



Yara detected Quasar RAT

Remote Access Functionality:

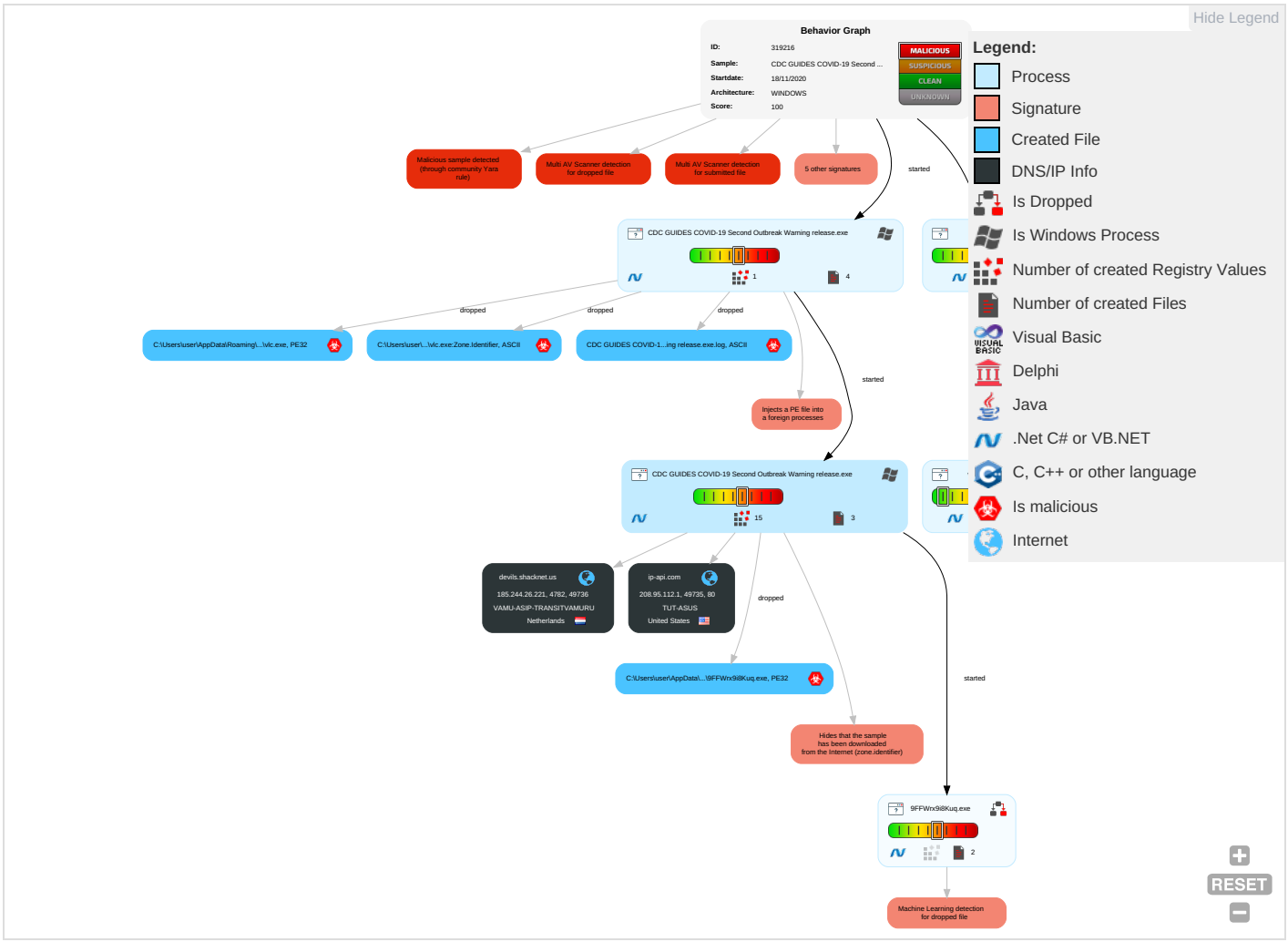


Yara detected Quasar RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co an
Valid Accounts	Windows Management Instrumentation 1 2 1	Registry Run Keys / Startup Folder 1 1	Process Injection 1 1 2	Disable or Modify Tools 1	Input Capture 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ing Tra
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	En Ch
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2 1	Security Account Manager	System Information Discovery 1 2 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	No Po
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2	NTDS	Security Software Discovery 2 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	No Ap La Pr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 4	SSH	Keylogging	Data Transfer Size Limits	Ap La Pr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 4	Cached Domain Credentials	Process Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mu Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap La
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	We
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fil Pr

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
CDC GUIDES COVID-19 Second Outbreak Warning release.exe	12%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\9FFWrx9i8Kuq.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	12%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
21.2.vlc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1135947		Download File
5.2.CDC GUIDES COVID-19 Second Outbreak Warning release.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1135947		Download File
20.2.vlc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1135947		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.m0odoca	0%	Avira URL Cloud	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://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	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://https://www.chiark.greenend.org.uk/~sgtatham/putty/0	0%	Avira URL Cloud	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://ip-api.com4	0%	Avira URL Cloud	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.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://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.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	
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.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.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ip-api.com	208.95.112.1	true	false		high
devils.shacknet.us	185.244.26.221	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ip-api.com/json/	false		high

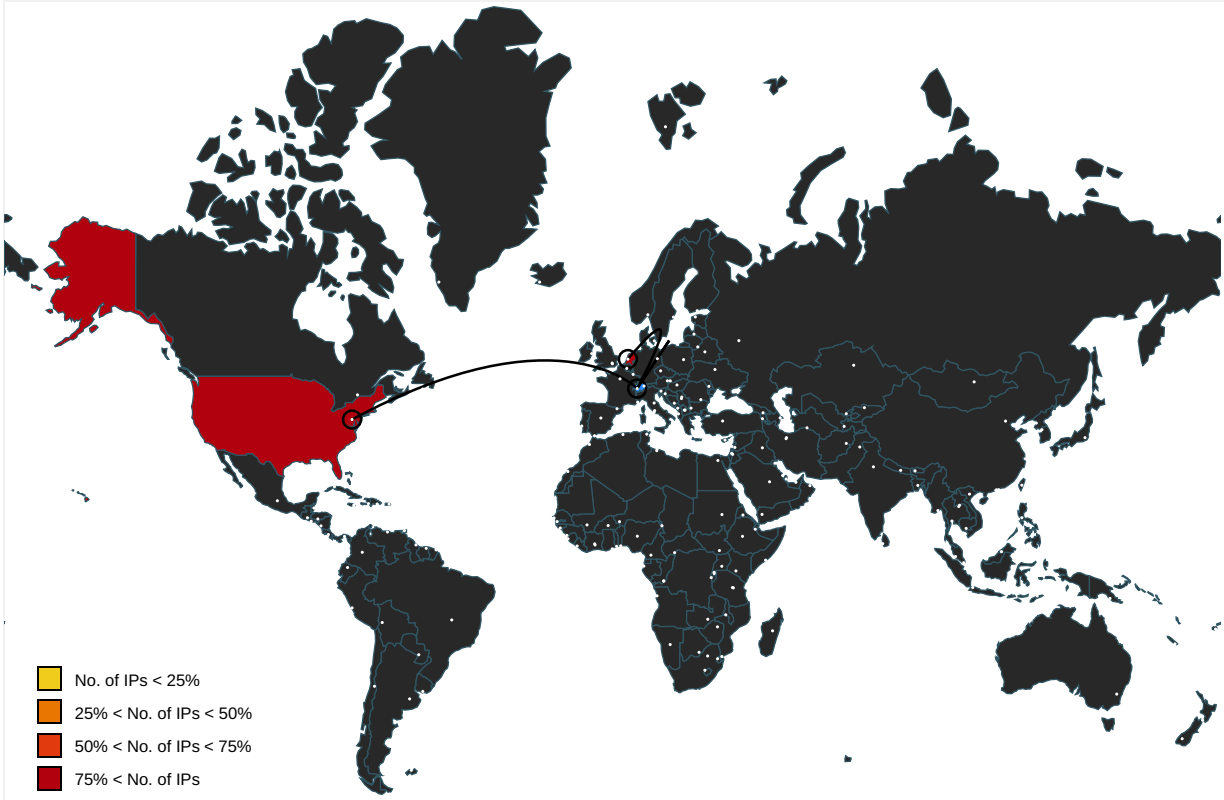
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false		high
http://freegeoip.net/xml/	CDC GUIDES COVID-19 Second Outbreak Warning release.exe, 00000000.00000002.267762525.00000000F82000.00000004.00000001.sdmp, CDC GUIDES COVID-19 Second Outbreak Warning release.exe, 00000005.00000002.831738365.000000000402000.00000040.00000001.sdmp, vlc.exe, 0000000E.00000002.353478457.0000000002A3F000.00000004.00000001.sdmp, vlc.exe, 0000000F.00000002.372076333.0000002E5F000.00000004.00000001.sdmp, vlc.exe, 00000014.00000002.358547843.000000000402000.00000040.00000001.sdmp, vlc.exe, 00000015.00000002.376779243.0000000000402000.00000040.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false		high
http://crl.m0odoca	CDC GUIDES COVID-19 Second Outbreak Warning release.exe, 00000005.00000002.839709535.000000031D9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.datacontract.org/2004/07/	CDC GUIDES COVID-19 Second Outbreak Warning release.exe, 00000005.00000002.837474746.00000002F23000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false		high
http://ocsp.thawte.com0	CDC GUIDES COVID-19 Second Outbreak Warning release.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.com	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.chiark.greenend.org.uk/~sgtatham/putty/0	CDC GUIDES COVID-19 Second Outbreak Warning release.exe, 00000005.00000002.839822026.00000003207000.00000004.00000001.sdmp, 9FFWrx9i8Kuq.exe.5.dr	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ip-api.com4	CDC GUIDES COVID-19 Second Outbreak Warning release.exe, 00000005.00000002.837102867.00000002EDC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	CDC GUIDES COVID-19 Second Outbreak Warning release.exe	false		high
http://www.jiyu-kobo.co.jp/	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ip-api.com	CDC GUIDES COVID-19 Second Outbreak Warning release.exe, 00000005.00000002.837102867.00000002EDC000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api.ipify.org/	CDC GUIDES COVID-19 Second Outbreak Warning release.exe, 00000000.00000002.267762525.00000002F82000.00000004.00000001.sdmp, CDC GUIDES COVID-19 Second Outbreak Warning release.exe, 00000005.00000002.831738365.0000000000402000.00000040.00000001.sdmp, vlc.exe, 0000000E.00000002.353478457.0000000002A3F000.00000004.00000001.sdmp, vlc.exe, 0000000F.00000002.372076333.0000000002E5F000.00000004.00000001.sdmp, vlc.exe, 00000014.00000002.358547843.0000000000402000.00000040.00000001.sdmp, vlc.exe, 00000015.00000002.376779243.0000000000402000.00000040.00000001.sdmp	false		high
http://www.fontbureau.com/designers8	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false		high
http://www.fonts.com	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CDC GUIDES COVID-19 Second Outbreak Warning release.exe, 00000005.00000002.837102867.00000002EDC000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	9FFWrx9i8Kuq.exe, 00000026.00000002.842466971.00000000063A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.95.112.1	unknown	United States		53334	TUT-ASUS	false
185.244.26.221	unknown	Netherlands		47158	VAMU-ASIP-TRANSITVAMURU	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	319216
Start date:	18.11.2020
Start time:	05:46:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CDC GUIDES COVID-19 Second Outbreak Warning release.scr (renamed file extension from scr to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	39
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

Copyright null 2020

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@11/5@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.7% (good quality ratio 0.4%) • Quality average: 47.1% • Quality standard deviation: 39.7%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, RuntimeBroker.exe, backgroundTaskHost.exe, UsoClient.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, MusNotifyIcon.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 104.43.139.144, 51.104.139.180, 2.20.84.85, 20.54.26.129, 2.20.142.210, 2.20.142.209, 92.122.213.194, 92.122.213.247, 52.155.217.156, 40.90.23.247, 40.90.137.127, 40.90.137.124, 40.90.23.154, 40.90.23.208, 13.104.215.69, 40.90.137.120, 40.90.137.126, 51.11.168.232 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, login.live.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, 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, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, login.msa.msidentity.com, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcolwus16.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 NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/319216/sample/CDC GUIDES COVID-19 Second Outbreak Warning release.exe

Simulations

Behavior and APIs

Time	Type	Description
05:48:17	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run vlc "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"
05:48:25	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
208.95.112.1	JfBrVoAbZJ.exe	Get hash	malicious	Browse	• ip-api.com/json/
	COMSurrogate.exe	Get hash	malicious	Browse	• ip-api.com/xml
	XbVizOmLp2.exe	Get hash	malicious	Browse	• ip-api.com/line/
	5GdTme5iYr.exe	Get hash	malicious	Browse	• ip-api.com/line/
	ASX9zO2dRS.exe	Get hash	malicious	Browse	• ip-api.com/json
	nW6wmlBvYs.exe	Get hash	malicious	Browse	• ip-api.com/line/
	58M6JBEHW4.exe	Get hash	malicious	Browse	• ip-api.com/json/
	wQDprpZ6i7.exe	Get hash	malicious	Browse	• ip-api.com/json/
	Xxgm9UF1xP.exe	Get hash	malicious	Browse	• ip-api.com/json/
	mY08H9Efjn.exe	Get hash	malicious	Browse	• ip-api.com/line/
	DHL Shipment Notice of Arrival AWB 8032697940773.js	Get hash	malicious	Browse	• ip-api.com/json/
	UuKzWnNMP6.exe	Get hash	malicious	Browse	• ip-api.com/json/
	xGaL85Q9T2.exe	Get hash	malicious	Browse	• ip-api.com/line/
	J7y5VaY5WM.exe	Get hash	malicious	Browse	• ip-api.com/line/
	M5tzeNIe5t.exe	Get hash	malicious	Browse	• ip-api.com/json/
	1LdcfAJXhM.exe	Get hash	malicious	Browse	• ip-api.com/json/
	hjeBW2gHjq.exe	Get hash	malicious	Browse	• ip-api.com/line/
	FOZUynGAgb.exe	Get hash	malicious	Browse	• ip-api.com/line/?fields
	s2VoGiX9ai.exe	Get hash	malicious	Browse	• ip-api.com/line/
	Bo0YWPrh0j.exe	Get hash	malicious	Browse	• ip-api.com/line/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ip-api.com	JfBrVoAbZJ.exe	Get hash	malicious	Browse	• 208.95.112.1
	COMSurrogate.exe	Get hash	malicious	Browse	• 208.95.112.1
	XbVizOmLp2.exe	Get hash	malicious	Browse	• 208.95.112.1
	5GdTme5iYr.exe	Get hash	malicious	Browse	• 208.95.112.1
	ASX9zO2dRS.exe	Get hash	malicious	Browse	• 208.95.112.1
	nW6wmlBvYs.exe	Get hash	malicious	Browse	• 208.95.112.1
	58M6JBEHW4.exe	Get hash	malicious	Browse	• 208.95.112.1
	wQDprpZ6i7.exe	Get hash	malicious	Browse	• 208.95.112.1
	Xxgm9UF1xP.exe	Get hash	malicious	Browse	• 208.95.112.1
	mY08H9Efjn.exe	Get hash	malicious	Browse	• 208.95.112.1
	DHL Shipment Notice of Arrival AWB 8032697940773.js	Get hash	malicious	Browse	• 208.95.112.1
	UuKzWnNMP6.exe	Get hash	malicious	Browse	• 208.95.112.1

Copyright null 2020

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	xGaL85Q9T2.exe	Get hash	malicious	Browse	• 208.95.112.1
	J7y5VaY5WM.exe	Get hash	malicious	Browse	• 208.95.112.1
	M5tzeNIe5t.exe	Get hash	malicious	Browse	• 208.95.112.1
	1LdcfAJXhM.exe	Get hash	malicious	Browse	• 208.95.112.1
	hjeBW2gHjq.exe	Get hash	malicious	Browse	• 208.95.112.1
	FOZUynGAgb.exe	Get hash	malicious	Browse	• 208.95.112.1
	s2VoGiX9ai.exe	Get hash	malicious	Browse	• 208.95.112.1
	Bo0YWPrh0j.exe	Get hash	malicious	Browse	• 208.95.112.1

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VAMU-ASIP-TRANSITVAMURU	85RNPseqgJ.exe	Get hash	malicious	Browse	• 185.244.26.206
	Olzcqxcxnf9.exe	Get hash	malicious	Browse	• 185.244.26.213
	R1MfM3z2Nz.exe	Get hash	malicious	Browse	• 185.244.26.206
	Fh06tuCZaK.exe	Get hash	malicious	Browse	• 185.244.26.206
	AITKG0L5d8.exe	Get hash	malicious	Browse	• 185.244.26.206
	Rbmmuoavjkz8.exe	Get hash	malicious	Browse	• 185.244.26.213
	PO 6300019918..exe	Get hash	malicious	Browse	• 185.244.26.206
	gSTnUDrWFe.exe	Get hash	malicious	Browse	• 185.244.26.199
	FpK385nmHk.exe	Get hash	malicious	Browse	• 185.244.26.199
	7sbXVpHq6E.exe	Get hash	malicious	Browse	• 185.244.26.199
	Order N#U00b022019.exe	Get hash	malicious	Browse	• 185.244.26.219
	scan.exe	Get hash	malicious	Browse	• 185.244.26.219
	3kpUlycHABfLMj6.exe	Get hash	malicious	Browse	• 185.244.26.228
	BTQBVILB.EXE	Get hash	malicious	Browse	• 185.244.26.228
	NCNRDEZ1.EXE	Get hash	malicious	Browse	• 185.244.26.228
	BM6GMIYN.EXE	Get hash	malicious	Browse	• 185.244.26.228
	QPI51NCL.EXE	Get hash	malicious	Browse	• 185.244.26.228
	LqyD3LqYjmUTl0n.exe	Get hash	malicious	Browse	• 185.244.26.228
	B6X9zW00qtAZXYd.exe	Get hash	malicious	Browse	• 185.244.26.228
	uPtScCCsvXI2Nj0.exe	Get hash	malicious	Browse	• 185.244.26.228
TUT-ASUS	JfBrVoAbZJ.exe	Get hash	malicious	Browse	• 208.95.112.1
	COMSurrogate.exe	Get hash	malicious	Browse	• 208.95.112.1
	XbVizOmLp2.exe	Get hash	malicious	Browse	• 208.95.112.1
	5GdTme5iYr.exe	Get hash	malicious	Browse	• 208.95.112.1
	nW6wmlBvYs.exe	Get hash	malicious	Browse	• 208.95.112.1
	58M6JBEHW4.exe	Get hash	malicious	Browse	• 208.95.112.1
	wQDprpZ6i7.exe	Get hash	malicious	Browse	• 208.95.112.1
	Xxgm9UF1xP.exe	Get hash	malicious	Browse	• 208.95.112.1
	mY08H9Efjn.exe	Get hash	malicious	Browse	• 208.95.112.1
	DHL Shipment Notice of Arrival AWB 8032697940773.js	Get hash	malicious	Browse	• 208.95.112.1
	UuKzWnNMP6.exe	Get hash	malicious	Browse	• 208.95.112.1
	xGaL85Q9T2.exe	Get hash	malicious	Browse	• 208.95.112.1
	J7y5VaY5WM.exe	Get hash	malicious	Browse	• 208.95.112.1
	M5tzeNIe5t.exe	Get hash	malicious	Browse	• 208.95.112.1
	1LdcfAJXhM.exe	Get hash	malicious	Browse	• 208.95.112.1
	hjeBW2gHjq.exe	Get hash	malicious	Browse	• 208.95.112.1
	FOZUynGAgb.exe	Get hash	malicious	Browse	• 208.95.112.1
	s2VoGiX9ai.exe	Get hash	malicious	Browse	• 208.95.112.1
	Bo0YWPrh0j.exe	Get hash	malicious	Browse	• 208.95.112.1
	UJr2wEBvsX.exe	Get hash	malicious	Browse	• 208.95.112.1

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

Copyright null 2020

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CDC GUIDES COVID-19 Second Outbreak Warning release.exe.log	
Process:	C:\Users\user\Desktop\CDC GUIDES COVID-19 Second Outbreak Warning release.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	517
Entropy (8bit):	5.335306720429945
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9l0ZKhaxzAbDLI4M6:ML9E4Ks2wKDE4KhK3VZ9pKhmsXE4j
MD5:	BB6624785B5CCCA1B27C160A2F19C179
SHA1:	51C3A976DB55F4E09009C1E7663643A2205FBEA5
SHA-256:	CF05D58CFF71D857664AAB4D49D3ABABFD0D59A65303B0FA5B1996C1CD3E66DA
SHA-512:	83C5B206F17844ECE6D3F8330C661A66C76803DF80BDD29780C541963D4693F89947407336D4CDE03F1F902C8F50B64E4F49C1577B99AAB09EDA16F1677CA843
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vlc.exe.log	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	517
Entropy (8bit):	5.335306720429945
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9l0ZKhaxzAbDLI4M6:ML9E4Ks2wKDE4KhK3VZ9pKhmsXE4j
MD5:	BB6624785B5CCCA1B27C160A2F19C179
SHA1:	51C3A976DB55F4E09009C1E7663643A2205FBEA5
SHA-256:	CF05D58CFF71D857664AAB4D49D3ABABFD0D59A65303B0FA5B1996C1CD3E66DA
SHA-512:	83C5B206F17844ECE6D3F8330C661A66C76803DF80BDD29780C541963D4693F89947407336D4CDE03F1F902C8F50B64E4F49C1577B99AAB09EDA16F1677CA843
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\9FFWrx9i8Kuq.exe	
Process:	C:\Users\user\Desktop\CDC GUIDES COVID-19 Second Outbreak Warning release.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	287120
Entropy (8bit):	4.744226336831956
Encrypted:	false
SSDEEP:	6144:ZL9q3/hFX11OUPKLIIjjGzIAh9+B2UTeZis7OiQGYH649Mwxz:J0/X11OUPK5jjSAB2UTKpOiQGYH3Mwxz
MD5:	082B27BB1AAA169A5D0C4CD536976F99
SHA1:	F0C3E75BDC2D2F57B1309F3A26FB99E67546012C
SHA-256:	A8886AF066529DB9AE1A07AE170DC1B80726952DE1094ED5E14520922DC47A54
SHA-512:	BD2175E9EDF2B314901904E4F0EB81C7969B2ADAD2F9033BC95B0F28ACDB2D2C15B9B2EE5A2D36D31D20A4066BF768012344001D1EF1FFE4641674C3C35F223
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...y.._.....'"... ...@....@.. ....@.....&..W....@.....$...=...`.....  .....  ..H.....text...(.... .....  .`.rsrc.....@.....@..@.rel oc.....`.....".....@..B.....'.....H.....$.....;...h4.....0.....-.&(....+.&+.*....0..h..... .....-.&~.....,.&+).+..+....(....r...p(.....-.&. ....Z.+..+.. .&..1..(.... .H... _.....Z...Y.. ....0.*.0.....-.&(....+.&+.*....0.....r...p.-.&+.(....+.*..0.....%.-.&9....+..+..r...p(....-B.r/..p(....-H.rA..p(....-N.rY..p(....-L.ri..p(....-J.r...p(....-H*r...p.- .&+.(....+.*r...p.-.&+.(....+.*r...p(....*r...p(....*r...p(....*r...p(....*....0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	
Process:	C:\Users\user\Desktop\CDC GUIDES COVID-19 Second Outbreak Warning release.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	645440
Entropy (8bit):	7.920263997977594
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	
SSDEEP:	12288:/4WN/IQY26pufbscH9POzQpGf2JUC5KJq7n8eUUI+PBUJXAXq:/Bb6ZcdOH2+CMJ2aiBUJXAXq
MD5:	DC8D9C9A86FE4830053697C1DC59DC6F
SHA1:	A63FA3CC878EFE75ECF849111C3E3D417FEF4FDD
SHA-256:	5DCD1649D97E0DA882778EC70677BE52B49603B6596B044518F02C278D93D0F2
SHA-512:	8F91ACA4B85D53745F395888FFB8E2D5F17F06AFC7E302F2ED19C840377C70EF807BA14748FEFD2A756B27B54808651087FBCBA572F0D162B06C8A0E9283EF8C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 12%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....b...D..... .....@.. ....@.....J.....@.....@1..... ....H.....text....a... ...b..... ..`.rsrc....@.....B...d.....@..@.relo c.....@..B.....H.....>.....h...e.....N+.+.*(....+.(....+..0..... ..a.%,[8....8....&8.... ....a%..^8....8.....Y.-..:v...E..... .. ..5...P.....+.8{... .{V.%,7Z ...&a.-.+m+.+I I.46Z ..p.a+a8.....(..... }.m.Z ..z.a.8m.... Z.}.Z (>.Ea.8Z....8T...(q...8O....8O....8X....8W....8.....+..+..+...(....*..(....*..(....*..(....*..(....*..(....*..(....*..(....*..(....*..(....*..(....*..(....*..(....*..(....*..(....*..(....*..(....*..(....*..(.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\CDC GUIDES COVID-19 Second Outbreak Warning release.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.920263997977594
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	CDC GUIDES COVID-19 Second Outbreak Warning release.exe
File size:	645440
MD5:	dc8d9c9a86fe4830053697c1dc59dc6f
SHA1:	a63fa3cc878efe75ecf849111c3e3d417fef4fdd
SHA256:	5dcd1649d97e0da882778ec70677be52b49603b6596b044518f02c278d93d0f2
SHA512:	8f91aca4b85d53745f395888ffb8e2d5f17f06afc7e302f2ed19c840377c70ef807ba14748fefd2a756b27b54808651087fbcba572f0d162b06c8a0e9283ef8c
SSDEEP:	12288:/4WN/IQY26pufbscH9POzQpGf2JUC5KJq7n8eUUI+PBUJXAXq:/Bb6ZcdOH2+CMJ2aiBUJXAXq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... ._.....b...D..... .....@.. ....@.....

File Icon



Icon Hash:	3b3b332b696932b2

Static PE Info

General

Entrypoint:	0x488117
Entrypoint Section:	.text
Digitally signed:	true
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:	0x5FB3FDCD [Tue Nov 17 16:43:57 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

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=GlobalSign CodeSigning CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 8/25/2020 6:42:07 AM 8/26/2023 6:42:07 AM
Subject Chain	• CN=win.rar GmbH, O=win.rar GmbH, L=Berlin, S=Berlin, C=DE
Version:	3
Thumbprint MD5:	185DBD4A2E2671589EEB3E7E1920EA9F
Thumbprint SHA-1:	B3DF816A17A25557316D181DDB9F46254D6D8CA0
Thumbprint SHA-256:	66DB1C86D38273627C837F4638122FA88BBFFFF31C4052115B98CAF6CE0C631E
Serial:	731D40AE3F3A1FB2BC3D8395

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

Instruction
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x880cd	0x4a	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8a000	0x14003	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x9a800	0x3140	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa0000	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	0x8611d	0x86200	False	0.959510426375	data	7.95282361002	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0x14003	0x14200	False	0.831982725155	data	7.61557514964	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa0000	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	0x8a09c	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x8a628	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x8aef4	0xea8	data		
RT_ICON	0x8bdc0	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x8c24c	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x8d318	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x8f8e4	0xd646	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0x9cf66	0x68	data		
RT_VERSION	0x9d00a	0x368	data		
RT_MANIFEST	0x9d3ae	0xc55	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

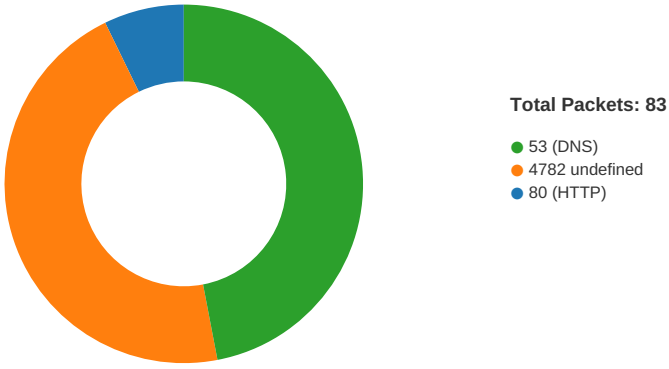
Imports

DLL	Import
mscoree.dll	_CorExeMain

Copyright null 2020

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 05:48:18.525491953 CET	49735	80	192.168.2.3	208.95.112.1
Nov 18, 2020 05:48:18.556354046 CET	80	49735	208.95.112.1	192.168.2.3
Nov 18, 2020 05:48:18.556437969 CET	49735	80	192.168.2.3	208.95.112.1
Nov 18, 2020 05:48:18.556812048 CET	49735	80	192.168.2.3	208.95.112.1
Nov 18, 2020 05:48:18.587726116 CET	80	49735	208.95.112.1	192.168.2.3
Nov 18, 2020 05:48:18.638310909 CET	49735	80	192.168.2.3	208.95.112.1
Nov 18, 2020 05:48:19.751044989 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:48:19.984572887 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:48:19.984734058 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:48:20.218857050 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:48:20.263480902 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:48:20.783591032 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:48:21.018487930 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:48:21.060591936 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:48:46.031399965 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:48:46.265988111 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:48:46.294056892 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:48:46.294157982 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:49:11.283453941 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:49:11.516608000 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:49:11.533206940 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:49:11.533683062 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:49:32.079123974 CET	80	49735	208.95.112.1	192.168.2.3
Nov 18, 2020 05:49:32.079448938 CET	49735	80	192.168.2.3	208.95.112.1
Nov 18, 2020 05:49:36.519959927 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:49:36.753957987 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:49:36.774738073 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:49:36.774939060 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:49:58.611615896 CET	49735	80	192.168.2.3	208.95.112.1
Nov 18, 2020 05:49:58.642582893 CET	80	49735	208.95.112.1	192.168.2.3
Nov 18, 2020 05:50:01.787627935 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:50:02.125547886 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:50:27.009057045 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:50:27.009284019 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:50:27.133411884 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:50:27.365962982 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:50:52.246691942 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:50:52.246948004 CET	49736	4782	192.168.2.3	185.244.26.221

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 05:50:52.373559952 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:50:52.606232882 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:51:17.475369930 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:51:17.475509882 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:51:17.610186100 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:51:17.842860937 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:51:42.710359097 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:51:42.710527897 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:51:42.846751928 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:51:43.079406023 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:07.948128939 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:07.948257923 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:08.083033085 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:08.315323114 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:33.186500072 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:33.188303947 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:33.320658922 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:33.552930117 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:35.871159077 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:35.871495008 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:35.871567011 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:35.871581078 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:35.871627092 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:35.871773005 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:36.104974985 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.105020046 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.105078936 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.105122089 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.105211020 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.105252981 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:36.105282068 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:36.105376005 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.105456114 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.105468988 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:36.105578899 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.105665922 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:36.339184999 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.339503050 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.339589119 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:36.339943886 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.340055943 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.340131998 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:36.340162992 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.340217113 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.340281963 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:36.340287924 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.340622902 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.340780973 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.340825081 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.340882063 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.340892076 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:36.340925932 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.340977907 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:36.341006041 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.341070890 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.341137886 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:36.341173887 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.341243982 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.341303110 CET	49736	4782	192.168.2.3	185.244.26.221
Nov 18, 2020 05:52:36.572417021 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.572464943 CET	4782	49736	185.244.26.221	192.168.2.3
Nov 18, 2020 05:52:36.572628021 CET	49736	4782	192.168.2.3	185.244.26.221

UDP Packets

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 05:47:50.012521982 CET	50141	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:47:50.048382998 CET	53	50141	8.8.8.8	192.168.2.3
Nov 18, 2020 05:47:51.043196917 CET	53023	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:47:51.070591927 CET	53	53023	8.8.8.8	192.168.2.3
Nov 18, 2020 05:47:52.042040110 CET	49563	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:47:52.069349051 CET	53	49563	8.8.8.8	192.168.2.3
Nov 18, 2020 05:47:52.983020067 CET	51352	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:47:53.010381937 CET	53	51352	8.8.8.8	192.168.2.3
Nov 18, 2020 05:47:53.781693935 CET	59349	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:47:53.809468031 CET	53	59349	8.8.8.8	192.168.2.3
Nov 18, 2020 05:47:56.386013985 CET	57084	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:47:56.413583040 CET	53	57084	8.8.8.8	192.168.2.3
Nov 18, 2020 05:47:59.936918020 CET	58823	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:47:59.964804888 CET	53	58823	8.8.8.8	192.168.2.3
Nov 18, 2020 05:48:01.808809042 CET	57568	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:48:01.844299078 CET	53	57568	8.8.8.8	192.168.2.3
Nov 18, 2020 05:48:02.866597891 CET	50540	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:48:02.893863916 CET	53	50540	8.8.8.8	192.168.2.3
Nov 18, 2020 05:48:05.870398998 CET	54366	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:48:05.897926092 CET	53	54366	8.8.8.8	192.168.2.3
Nov 18, 2020 05:48:05.942739964 CET	53034	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:48:05.970174074 CET	53	53034	8.8.8.8	192.168.2.3
Nov 18, 2020 05:48:06.722620010 CET	57762	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:48:06.750351906 CET	53	57762	8.8.8.8	192.168.2.3
Nov 18, 2020 05:48:09.962953091 CET	55435	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:48:09.990643024 CET	53	55435	8.8.8.8	192.168.2.3
Nov 18, 2020 05:48:11.889908075 CET	50713	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:48:11.917452097 CET	53	50713	8.8.8.8	192.168.2.3
Nov 18, 2020 05:48:12.983668089 CET	56132	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:48:13.011457920 CET	53	56132	8.8.8.8	192.168.2.3
Nov 18, 2020 05:48:14.170641899 CET	58987	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:48:14.222070932 CET	53	58987	8.8.8.8	192.168.2.3
Nov 18, 2020 05:48:18.481765032 CET	56579	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:48:18.509390116 CET	53	56579	8.8.8.8	192.168.2.3
Nov 18, 2020 05:48:19.676497936 CET	60633	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:48:19.720848083 CET	53	60633	8.8.8.8	192.168.2.3
Nov 18, 2020 05:48:20.004332066 CET	61292	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:48:20.032116890 CET	53	61292	8.8.8.8	192.168.2.3
Nov 18, 2020 05:48:29.786113024 CET	63619	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:48:29.824052095 CET	53	63619	8.8.8.8	192.168.2.3
Nov 18, 2020 05:48:39.943408012 CET	64938	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:48:39.971239090 CET	53	64938	8.8.8.8	192.168.2.3
Nov 18, 2020 05:48:42.993231058 CET	61946	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:48:43.030543089 CET	53	61946	8.8.8.8	192.168.2.3
Nov 18, 2020 05:49:14.649454117 CET	64910	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:49:14.677381039 CET	53	64910	8.8.8.8	192.168.2.3
Nov 18, 2020 05:49:15.810158968 CET	52123	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:49:15.854407072 CET	53	52123	8.8.8.8	192.168.2.3
Nov 18, 2020 05:50:30.843565941 CET	56130	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:50:30.895143986 CET	53	56130	8.8.8.8	192.168.2.3
Nov 18, 2020 05:50:31.429007053 CET	56338	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:50:31.467190981 CET	53	56338	8.8.8.8	192.168.2.3
Nov 18, 2020 05:50:31.871423006 CET	59420	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:50:31.907816887 CET	53	59420	8.8.8.8	192.168.2.3
Nov 18, 2020 05:50:32.373737097 CET	58784	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:50:32.422290087 CET	53	58784	8.8.8.8	192.168.2.3
Nov 18, 2020 05:50:32.810376883 CET	63978	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:50:32.845983982 CET	53	63978	8.8.8.8	192.168.2.3
Nov 18, 2020 05:50:33.219400883 CET	62938	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:50:33.255281925 CET	53	62938	8.8.8.8	192.168.2.3
Nov 18, 2020 05:50:33.778590918 CET	55708	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:50:33.814464092 CET	53	55708	8.8.8.8	192.168.2.3
Nov 18, 2020 05:50:34.817584991 CET	56803	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:50:34.853290081 CET	53	56803	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 05:50:35.515963078 CET	57145	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:50:35.551986933 CET	53	57145	8.8.8.8	192.168.2.3
Nov 18, 2020 05:50:35.847608089 CET	55359	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:50:35.874603033 CET	53	55359	8.8.8.8	192.168.2.3
Nov 18, 2020 05:52:31.505094051 CET	58306	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:52:31.542376995 CET	53	58306	8.8.8.8	192.168.2.3
Nov 18, 2020 05:52:32.180982113 CET	64124	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:52:32.226928949 CET	53	64124	8.8.8.8	192.168.2.3
Nov 18, 2020 05:52:35.734662056 CET	49361	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:52:35.778562069 CET	53	49361	8.8.8.8	192.168.2.3
Nov 18, 2020 05:52:38.909137964 CET	63150	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:52:38.944977999 CET	53	63150	8.8.8.8	192.168.2.3
Nov 18, 2020 05:52:39.208183050 CET	53279	53	192.168.2.3	8.8.8.8
Nov 18, 2020 05:52:39.244232893 CET	53	53279	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 18, 2020 05:48:18.481765032 CET	192.168.2.3	8.8.8.8	0xda1d	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)
Nov 18, 2020 05:48:19.676497936 CET	192.168.2.3	8.8.8.8	0x43a3	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 18, 2020 05:48:18.509390116 CET	8.8.8.8	192.168.2.3	0xda1d	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)
Nov 18, 2020 05:48:19.720848083 CET	8.8.8.8	192.168.2.3	0x43a3	No error (0)	devils.shacknet.us		185.244.26.221	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ip-api.com

HTTP Packets

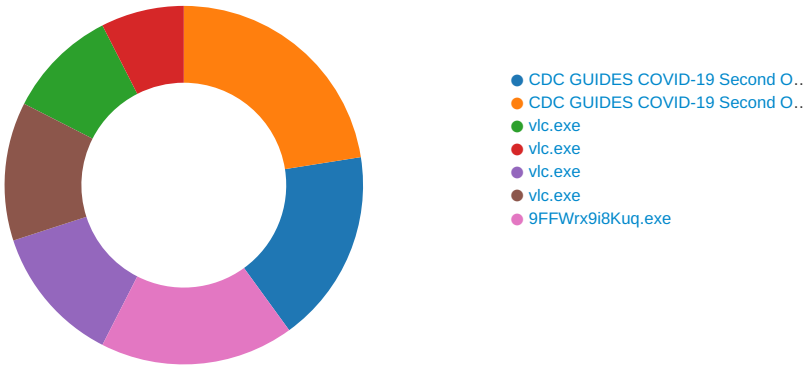
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49735	208.95.112.1	80	C:\Users\user\Desktop\CDC GUIDES COVID-19 Second Outbreak Warning release.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 05:48:18.556812048 CET	339	OUT	GET /json/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0 Host: ip-api.com Connection: Keep-Alive
Nov 18, 2020 05:48:18.587726116 CET	339	IN	HTTP/1.1 200 OK Date: Wed, 18 Nov 2020 04:48:17 GMT Content-Type: application/json; charset=utf-8 Content-Length: 281 Access-Control-Allow-Origin: * X-Ttl: 60 X-Rl: 44 Data Raw: 7b 22 73 74 61 74 75 73 22 3a 22 73 75 63 63 65 73 73 22 2c 22 63 6f 75 6e 74 72 79 22 3a 22 53 77 69 74 7a 65 72 6c 61 6e 64 22 2c 22 63 6f 75 6e 74 72 79 43 6f 64 65 22 3a 22 43 48 22 2c 22 72 65 67 69 6f 6e 22 3a 22 5a 48 22 2c 22 72 65 67 69 6f 6e 4e 61 6d 65 22 3a 22 5a 75 72 69 63 68 22 2c 22 63 69 74 79 22 3a 22 5a 75 72 69 63 68 22 2c 22 7a 69 70 22 3a 22 38 31 35 32 22 2c 22 6c 61 74 22 3a 34 37 2e 34 33 2c 22 6c 6f 6e 22 3a 38 2e 35 37 31 38 2c 22 74 69 6d 65 7a 6f 6e 65 22 3a 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 22 69 73 70 22 3a 22 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 22 2c 22 6f 72 67 22 3a 22 43 64 6e 37 37 20 5a 55 52 20 49 54 58 22 2c 22 61 73 22 3a 22 41 53 36 30 30 36 38 20 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 22 2c 22 71 75 65 72 79 22 3a 22 38 34 2e 31 37 2e 35 32 2e 34 30 22 7d Data Ascii: {"status":"success","country":"Switzerland","countryCode":"CH","region":"ZH","regionName":"Zurich","city":"Zurich","zip":"8152","lat":47.43,"lon":8.5718,"timezone":"Europe/Zurich","isp":"Datacamp Limited","org":"Cdn77 ZUR ITX","as":"AS60068 Datacamp Limited","query":"84.17.52.40"}

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: CDC GUIDES COVID-19 Second Outbreak Warning release.exe PID: 2764 Parent PID: 5664

General

Start time:	05:47:44
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\CDC GUIDES COVID-19 Second Outbreak Warning release.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CDC GUIDES COVID-19 Second Outbreak Warning release.exe'
Imagebase:	0xb40000
File size:	645440 bytes
MD5 hash:	DC8D9C9A86FE4830053697C1DC59DC6F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000000.00000002.269160984.0000000004035000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000000.00000002.269160984.0000000004035000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CE4BEFF	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	617C8D3	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	617C8D3	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CDC GUIDES COVID-19 Second Outbreak Warning release.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E30C78D	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CDC GUIDES COVID-19 Second Outbreak Warning release.exe.log	unknown	517	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0	success or wait	1	6E30C907	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	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	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	6CE4646A	RegSetValueExW

Analysis Process: CDC GUIDES COVID-19 Second Outbreak Warning release.exe PID: 5820 Parent PID: 2764

General

Start time:	05:48:15
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\CDC GUIDES COVID-19 Second Outbreak Warning release.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\CDC GUIDES COVID-19 Second Outbreak Warning release.exe
Imagebase:	0xb00000

File size:	645440 bytes
MD5 hash:	DC8D9C9A86FE4830053697C1DC59DC6F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000005.00000002.831738365.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000005.00000002.831738365.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
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	6DFFCF06	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	6DFFCF06	unknown
C:\Users\user\AppData\Local\Temp\9FFWrx9i8Kuq.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CE41E60	CreateFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\9FFWrx9i8Kuq.exe	unknown	65535	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\9FFWrx9i8Kuq.exe	unknown	65535	31 32 65 5e 34 61 39 62 62 36 62 35 33 39 33 37 31 5e 65 5e 38 5e 36 37 61 62 36 33 61 33 38 31 37 35 38 30 34 64 36 37 33 33 61 34 36 64 30 30 39 36 33 61 64 62 39 65 36 38 32 36 33 37 61 66 62 31 36 61 35 39 33 37 64 66 34 38 36 65 35 30 61 62 30 32 35 65 30 64 30 35 32 34 62 62 34 39 37 62 64 33 62 36 32 35 62 37 62 62 36 33 62 38 62 37 66 34 31 61 39 64 66 38 38 64 66 30 62 66 38 33 38 62 39 36 5e 39 36 39 35 38 32 36 38 31 64 5e 64 36 34 30 36 33 66 33 65 33 34 31 65 65 5e 36 64 33 36 35 64 64 31 66 30 30 31 30 62 32 61 33 31 37 31 37 36 35 66 65 34 35 32 30 34 37 66 65 33 30 34 35 65 32 65 34 38 66 65 39 5e 37 66 66 32 65 38 61 37 36 65 36 66 61 37 39 32 39 61 30 65 33 31 64 5e 31 66 61 65 31 34 37 37 38 38 36 30 36 35 33 34 31 5e 34 65 66 34 33 64	12e^4a9bb6b539371^e^8^67ab63a3 8175804d6733a46d00963adb9e6826 37afb16a5937df486e50ab025e0d05 24bb497bd3b625b7bb63b8b7f41a9d f88df0bf838b96^969582681d^d640 63f3e341ee^6d365dd1f0010b2a317 1765fe452047fe3045e2e48fe9^7ff 2e8a76e6fa7929a0e31d^1fae1477886065341^4ef43d	success or wait	4	6CE41B4F	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	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: vlc.exe PID: 6588 Parent PID: 3388

General

Start time:	05:48:25
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:	0x340000
File size:	645440 bytes
MD5 hash:	DC8D9C9A86FE4830053697C1DC59DC6F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 0000000E.00000002.355201046.00000000037C5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 0000000E.00000002.355201046.00000000037C5000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 12%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vlc.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E30C78D	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	517	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0	success or wait	1	6E30C907	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	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile

Analysis Process: vlc.exe PID: 6824 Parent PID: 3388

General

Start time:	05:48:34
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:	0x600000
File size:	645440 bytes
MD5 hash:	DC8D9C9A86FE4830053697C1DC59DC6F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 0000000F.00000002.372345849.0000000003BE5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 0000000F.00000002.372345849.0000000003BE5000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile

Analysis Process: vlc.exe PID: 2172 Parent PID: 6588

General

Start time:	05:48:54
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:	0xdf0000
File size:	645440 bytes
MD5 hash:	DC8D9C9A86FE4830053697C1DC59DC6F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000014.00000002.358547843.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000014.00000002.358547843.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
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	6DFFCF06	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	6DFFCF06	unknown

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	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile

Analysis Process: vlc.exe PID: 4080 Parent PID: 6824

General

Start time:	05:49:03
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:	0xca0000
File size:	645440 bytes
MD5 hash:	DC8D9C9A86FE4830053697C1DC59DC6F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000015.00000002.376779243.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000015.00000002.376779243.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
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	6DFFCF06	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	6DFFCF06	unknown

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	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile

Analysis Process: 9FFWrx9i8Kuq.exe PID: 496 Parent PID: 5820

General

Start time:	05:52:36
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Local\Temp\9FFWrx9i8Kuq.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\9FFWrx9i8Kuq.exe
Imagebase:	0xf20000
File size:	287120 bytes
MD5 hash:	082B27BB1AAA169A5D0C4CD536976F99
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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	6DFFCF06	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	6DFFCF06	unknown

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	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile

Disassembly

Code Analysis

Copyright null 2020