ID: 319976
Sample Name: COVID-19 CDC Secon Outbreak Warning release.scr
Cookbook: default.jbs
Time: 22:01:38
Date: 18/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

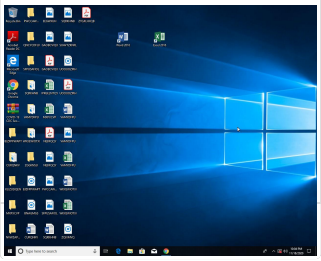
Analysis Report COVID-19 CDC Secon Outbreak Warnin…

Overview

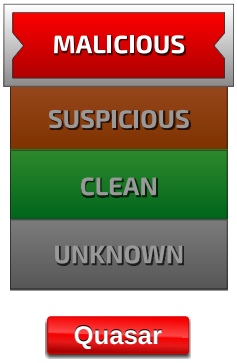
General Information

Sample Name:	COVID-19 CDC Secon Outbreak Warning release.scr (renamed file extension from scr to exe)
Analysis ID:	319976
MD5:	db0d632b83738d..
SHA1:	2f9269bfc05473a..
SHA256:	6fb60c80bdc9cd5..
Tags:	QuasarRAT scr

Most interesting Screenshot:



Detection

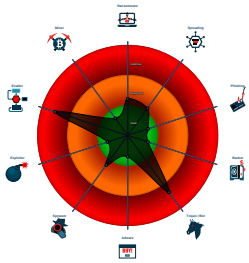


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Machine Learning detection for samp…
- May check the online IP address of …
- Queries sensitive BIOS Information …
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- COVID-19 CDC Secon Outbreak Warning release.exe (PID: 5856 cmdline: 'C:\Users\user\Desktop\COVID-19 CDC Secon Outbreak Warning release.exe' MD5: DB0D632B83738DFC64013B9B5B7C339E)
  - COVID-19 CDC Secon Outbreak Warning release.exe (PID: 7040 cmdline: C:\Users\user\Desktop\COVID-19 CDC Secon Outbreak Warning release.exe MD5: DB0D632B83738DFC64013B9B5B7C339E)
- winrar.exe (PID: 6972 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe' MD5: DB0D632B83738DFC64013B9B5B7C339E)
  - winrar.exe (PID: 5256 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe MD5: DB0D632B83738DFC64013B9B5B7C339E)
- winrar.exe (PID: 4576 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe' MD5: DB0D632B83738DFC64013B9B5B7C339E)
  - winrar.exe (PID: 5572 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe MD5: DB0D632B83738DFC64013B9B5B7C339E)
  - winrar.exe (PID: 5576 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe MD5: DB0D632B83738DFC64013B9B5B7C339E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.827897659.0000000000402000.00000040.00000001.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
0000000F.00000002.827897659.0000000000402000.00000040.00000001.sdmp	JoeSecurity_Quasar	Yara detected Quasar RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.822302365.00000000040E1000.00000004.00000001.sdmp	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x42657:$s1: DoUploadAndExecute • 0x99477:$s1: DoUploadAndExecute • 0x4289b:$s2: DoDownloadAndExecute • 0x996bb:$s2: DoDownloadAndExecute • 0x4241c:$s3: DoShellExecute • 0x9923c:$s3: DoShellExecute • 0x42853:$s4: set_Processname • 0x99673:$s4: set_Processname • 0x9f54:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x60d74:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x9e78:$op2: 00 17 03 1F 20 17 19 15 28 • 0x60c98:$op2: 00 17 03 1F 20 17 19 15 28 • 0xa8de:$op3: 00 04 03 69 91 1B 40 • 0xb12e:$op3: 00 04 03 69 91 1B 40 • 0x616fe:$op3: 00 04 03 69 91 1B 40 • 0x61f4e:$op3: 00 04 03 69 91 1B 40
00000009.00000002.822302365.00000000040E1000.00000004.00000001.sdmp	JoeSecurity_Quasar	Yara detected Quasar RAT	Joe Security	
00000003.00000002.924590953.0000000000402000.00000040.00000001.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 15 entries				

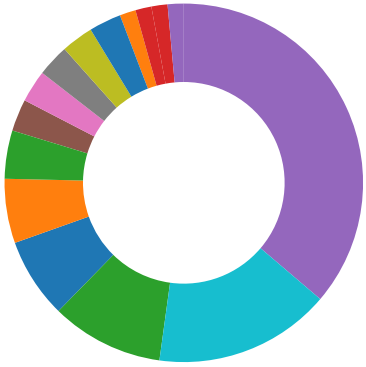
Unpacked PEs

Source	Rule	Description	Author	Strings
15.2.winrar.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:$s7: xClient.Core.ReverseProxy.Packets
15.2.winrar.exe.400000.0.unpack	xRAT_1	Detects Patchwork malware	Florian Roth	• 0x305c0:$x4: xClient.Properties.Resources.resources • 0x30481:$s4: Client.exe • 0x3e163:$s7: set_RunHidden
15.2.winrar.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
15.2.winrar.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
15.2.winrar.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
- 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
- Machine Learning detection for sample

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

Copyright null 2020

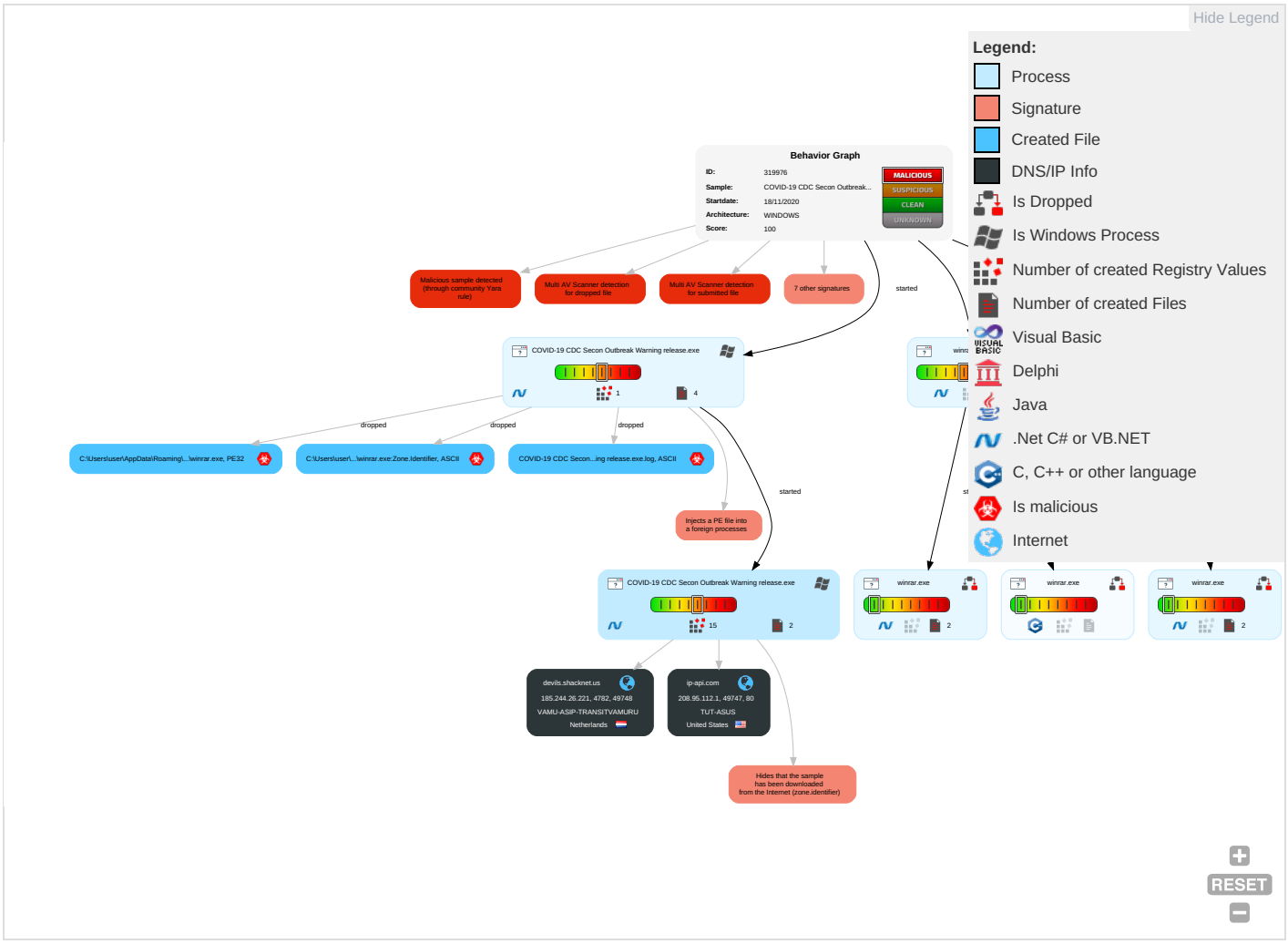
Remote Access Functionality:

Yara detected Quasar RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co ar
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	OS Credential Dumping	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	In Tr
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	Data from Removable Media	Exfiltration Over Bluetooth	Ex 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 2	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	W
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

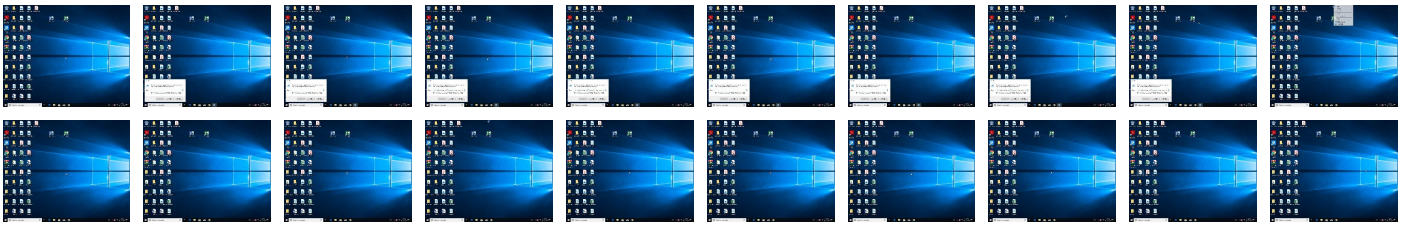
Behavior Graph



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
COVID-19 CDC Secon Outbreak Warning release.exe	53%	Virustotal		Browse
COVID-19 CDC Secon Outbreak Warning release.exe	14%	Metadefender		Browse
COVID-19 CDC Secon Outbreak Warning release.exe	59%	ReversingLabs	ByteCode-MSIL.Trojan.NanoBot	
COVID-19 CDC Secon Outbreak Warning release.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe	53%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe	14%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe	59%	ReversingLabs	ByteCode-MSIL.Trojan.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.2.winrar.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1135947		Download File
3.2.COVID-19 CDC Secon Outbreak Warning release.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1135947		Download File
13.2.winrar.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1135947		Download File

Copyright null 2020

Domains

Source	Detection	Scanner	Label	Link
devils.shacknet.us	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ip-api.com4Ck	0%	Avira URL Cloud	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://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://ocsp.thawte.com0	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	• 1%, Virustotal, Browse	unknown

Contacted URLs

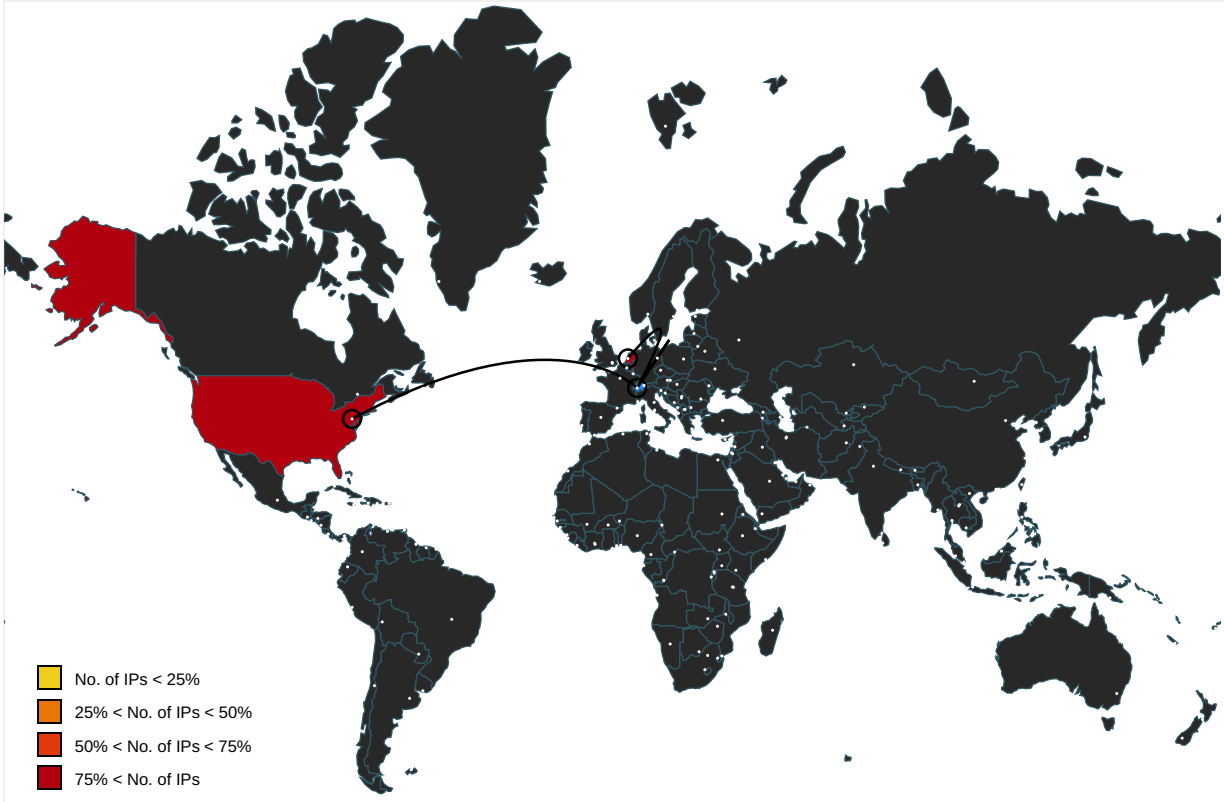
Name	Malicious	Antivirus Detection	Reputation
http://ip-api.com/json/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://api.ipify.org/	COVID-19 CDC Secon Outbreak Warning release.exe, 00000000.00000002.730193991.0000000002E97000.00000004.00000001.sdmp, COVID-19 CDC Secon Outbreak Warning release.exe, 00000003.00000002.924590953.0000000000402000.00000040.00000001.sdmp, winrar.exe, 00000005.00000002.807724606.0000000003528000.00000004.00000001.sdmp, winrar.exe, 00000009.00000002.822302365.00000000040E1000.00000004.00000001.sdmp, winrar.exe, 0000000D.00000002.808322166.0000000000402000.00000040.00000001.sdmp, winrar.exe, 0000000F.00000002.827897659.0000000000402000.00000040.00000001.sdmp	false		high
http://ip-api.com4Ck	COVID-19 CDC Secon Outbreak Warning release.exe, 00000003.00000002.925435864.000000000329C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://freegeoip.net/xml/	COVID-19 CDC Secon Outbreak Warning release.exe, 00000000.000000002.730193991.0000000002E97000.00000004.00000001.sdmp, COVID-19 CDC Secon Outbreak Warning release.exe, 00000003.00000002.924590953.0000000000402000.00000040.00000001.sdmp, winrar.exe, 00000005.00000002.807724606.0000000003528000.00000004.00000001.sdmp, winrar.exe, 00000009.00000002.822302365.00000000040E1000.00000004.00000001.sdmp, winrar.exe, 0000000D.00000002.808322166.0000000000402000.00000040.00000001.sdmp, winrar.exe, 0000000F.00000002.827897659.0000000000402000.00000040.00000001.sdmp	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	COVID-19 CDC Secon Outbreak Warning release.exe	false		high
http://schemas.datacontract.org/2004/07/	COVID-19 CDC Secon Outbreak Warning release.exe, 00000003.00000002.925473782.00000000032E3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	COVID-19 CDC Secon Outbreak Warning release.exe, 00000003.00000002.925435864.000000000329C000.00000004.00000001.sdmp	false		high
http://ocsp.thawte.com0	COVID-19 CDC Secon Outbreak Warning release.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ip-api.com	COVID-19 CDC Secon Outbreak Warning release.exe, 00000003.00000002.925435864.000000000329C000.00000004.00000001.sdmp	false		high

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

Copyright null 2020

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	319976
Start date:	18.11.2020
Start time:	22:01:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	COVID-19 CDC Secon 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:	18
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@11/4@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.8% (good quality ratio 0.6%) • Quality average: 50.5% • Quality standard deviation: 38.3%
HCA Information:	• Successful, ratio: 97% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.43.193.48, 51.104.139.180, 52.155.217.156, 20.54.26.129, 67.26.137.254, 67.26.83.254, 8.241.11.126, 8.253.204.249, 8.253.204.121, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.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, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net • 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.

Simulations

Behavior and APIs

Time	Type	Description
22:02:59	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run winrar "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe"
22:03:07	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run winrar "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.95.112.1	50139_GJO.msi	Get hash	malicious	Browse	• ip-api.com/json/
	accaf1b5618d15f665ee933d2684e82f.exe	Get hash	malicious	Browse	• ip-api.com/line/
	q4W2doW0OZ.exe	Get hash	malicious	Browse	• ip-api.com/json
	CDC GUIDES COVID-19 Second Outbreak Warning release.exe	Get hash	malicious	Browse	• ip-api.com/json/
	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/
185.244.26.221	CDC GUIDES COVID-19 Second Outbreak Warning release.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ip-api.com	50139_GJO.msi	Get hash	malicious	Browse	• 208.95.112.1
	accaf1b5618d15f665ee933d2684e82f.exe	Get hash	malicious	Browse	• 208.95.112.1
	q4W2doW0OZ.exe	Get hash	malicious	Browse	• 208.95.112.1

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	CDC GUIDES COVID-19 Second Outbreak Warning releas e.exe	Get hash	malicious	Browse	• 208.95.112.1
	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
	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
devils.shacknet.us	CDC GUIDES COVID-19 Second Outbreak Warning releas e.exe	Get hash	malicious	Browse	• 185.244.26.221

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VAMU-ASIP-TRANSITVAMURU	Kaszfnrcg7.exe	Get hash	malicious	Browse	• 185.244.26.213
	Inv No.5200003959 (FL).exe	Get hash	malicious	Browse	• 185.244.26.247
	CDC GUIDES COVID-19 Second Outbreak Warning releas e.exe	Get hash	malicious	Browse	• 185.244.26.221
	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
TUT-ASUS	50139_GJO.msi	Get hash	malicious	Browse	• 208.95.112.1
	accaf1b5618d15f665ee933d2684e82f.exe	Get hash	malicious	Browse	• 208.95.112.1
	q4W2doW0OZ.exe	Get hash	malicious	Browse	• 208.95.112.1
	CDC GUIDES COVID-19 Second Outbreak Warning releas e.exe	Get hash	malicious	Browse	• 208.95.112.1
	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

Copyright null 2020

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	hjeBW2gHjq.exe	Get hash	malicious	Browse	• 208.95.112.1

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\COVID-19 CDC Secon Outbreak Warning release.exe.log	
Process:	C:\Users\user\Desktop\COVID-19 CDC Secon 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/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhaxzAbDLI4M6: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\winrar.exe.log	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	517
Entropy (8bit):	5.335306720429945
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhaxzAbDLI4M6: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\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe	
Process:	C:\Users\user\Desktop\COVID-19 CDC Secon Outbreak Warning release.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	634176
Entropy (8bit):	7.917866889273155
Encrypted:	false
SSDEEP:	12288:4pwAe1+dbJ1wD7wBvn7pGxp+46IFBqmzKxBUJXA+:wLe1+dbJ1wQhtg1iBUJXA+
MD5:	DB0D632B83738DFC64013B9B5B7C339E
SHA1:	2F9269BFC05473A6DCE71C56D25B37D8B5490BCD
SHA-256:	6FB60C80BDC9CD558A384B468DC8B8467FB2E02764728E6A0EBC28CA865F31F6
SHA-512:	F35A95B4F1E31049AD9599D111F0F4E3E1422F98F8D539B6E9AB7327B1020A691026BD37CF7FAC090DB2AB810A8F9C471063BF5447FD63DBBF68F270825AA9CA

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe	
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 53%, Browse • Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 59%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...a[._.....B...8.....:`... .....@.. ..... ..@.....\_..J.....5.....|..@1..... ..... ..H.....text...@@... ...B..... ..`.rsrc....5.....6...D.....@..@.rel oc.....z.....@..B..... `.....H.....B.....(.....N+.+.*(....+..0..V.....8....8.... U.f.8....8.... P.f.8....9....&8....8....8.....o.....o.... ..f.(|...o.....,..o..... .f.(|....o....(..... U.f.(|..(.....o.....o.....s.....o.....,..o.....,..o.....,..o.....(..... .f.(|.....o....(.....(....&*.8....(....8....(|...8.....8....(|...8.....8.... ..8.....8....(....8.....L....B..Z.....;.+f..3.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\COVID-19 CDC Secon 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):	7.917866889273155
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:	COVID-19 CDC Secon Outbreak Warning release.exe
File size:	634176
MD5:	db0d632b83738dfc64013b9b5b7c339e
SHA1:	2f9269bfc05473a6dce71c56d25b37d8b5490bcd
SHA256:	6fb60c80bdc9cd558a384b468dc8b8467fb2e02764728e6a0ebc28ca865f31f6
SHA512:	f35a95b4f1e31049ad9599d111f0f4e3e1422f98f8d539b6e9ab7327b1020a691026bd37cf7fac090db2ab810a8f9c471063bf5447fd63dbbf68f270825aa9ca
SSDEEP:	12288:4pwAe1+dbJ1wD7wBvn7pGxp+46IFBqmzKxBUJXA+:wLe1+dbJ1wQhtg1iBUJXA+
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...a[._.....B...8.....:`... .....@.. .....@.....

File Icon

Icon Hash:	3b3b332b696932b2

Static PE Info

General	
Entrypoint:	0x48603a
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:	0x5FB35B61 [Tue Nov 17 05:10:57 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 3:42:07 PM 8/26/2023 3:42:07 PM
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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Copyright null 2020

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
add byte ptr [eax], al

Copyright null 2020

Instruction
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	0x85ff0	0x4a	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x88000	0x13590	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x97c00	0x3140	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9c000	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	0x84040	0x84200	False	0.957613307119	data	7.94855371176	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x88000	0x13590	0x13600	False	0.85138608871	data	7.63155477621	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

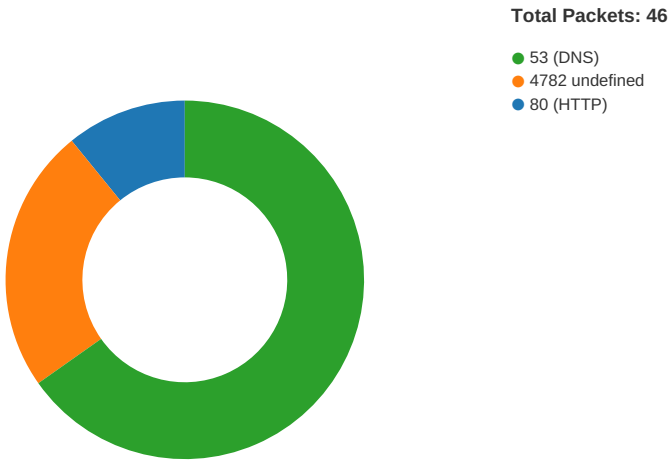
Name	RVA	Size	Type	Language	Country
RT_ICON	0x8809c	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x88628	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x88ef4	0xea8	data		
RT_ICON	0x89dc0	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x8a24c	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x8b318	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x8d8e4	0xd646	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0x9af66	0x68	data		
RT_VERSION	0x9b00a	0x360	data		
RT_MANIFEST	0x9b3a6	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 22:03:06.486851931 CET	49747	80	192.168.2.4	208.95.112.1
Nov 18, 2020 22:03:06.517319918 CET	80	49747	208.95.112.1	192.168.2.4
Nov 18, 2020 22:03:06.519470930 CET	49747	80	192.168.2.4	208.95.112.1
Nov 18, 2020 22:03:06.519504070 CET	49747	80	192.168.2.4	208.95.112.1
Nov 18, 2020 22:03:06.590480089 CET	80	49747	208.95.112.1	192.168.2.4
Nov 18, 2020 22:03:06.609174013 CET	80	49747	208.95.112.1	192.168.2.4
Nov 18, 2020 22:03:06.740864038 CET	49747	80	192.168.2.4	208.95.112.1
Nov 18, 2020 22:03:07.506920099 CET	49748	4782	192.168.2.4	185.244.26.221
Nov 18, 2020 22:03:07.739882946 CET	4782	49748	185.244.26.221	192.168.2.4
Nov 18, 2020 22:03:07.740027905 CET	49748	4782	192.168.2.4	185.244.26.221
Nov 18, 2020 22:03:07.975766897 CET	4782	49748	185.244.26.221	192.168.2.4
Nov 18, 2020 22:03:08.131855965 CET	49748	4782	192.168.2.4	185.244.26.221
Nov 18, 2020 22:03:09.252739906 CET	49748	4782	192.168.2.4	185.244.26.221
Nov 18, 2020 22:03:09.486231089 CET	4782	49748	185.244.26.221	192.168.2.4
Nov 18, 2020 22:03:09.631756067 CET	49748	4782	192.168.2.4	185.244.26.221
Nov 18, 2020 22:03:34.495062113 CET	49748	4782	192.168.2.4	185.244.26.221
Nov 18, 2020 22:03:34.727848053 CET	4782	49748	185.244.26.221	192.168.2.4
Nov 18, 2020 22:03:34.880531073 CET	4782	49748	185.244.26.221	192.168.2.4
Nov 18, 2020 22:03:34.883851051 CET	49748	4782	192.168.2.4	185.244.26.221
Nov 18, 2020 22:03:59.745313883 CET	49748	4782	192.168.2.4	185.244.26.221
Nov 18, 2020 22:03:59.977499008 CET	4782	49748	185.244.26.221	192.168.2.4
Nov 18, 2020 22:04:00.114784956 CET	4782	49748	185.244.26.221	192.168.2.4
Nov 18, 2020 22:04:00.114859104 CET	49748	4782	192.168.2.4	185.244.26.221
Nov 18, 2020 22:04:24.862526894 CET	80	49747	208.95.112.1	192.168.2.4
Nov 18, 2020 22:04:24.862608910 CET	49747	80	192.168.2.4	208.95.112.1
Nov 18, 2020 22:04:24.981982946 CET	49748	4782	192.168.2.4	185.244.26.221
Nov 18, 2020 22:04:25.215270042 CET	4782	49748	185.244.26.221	192.168.2.4
Nov 18, 2020 22:04:25.352879047 CET	4782	49748	185.244.26.221	192.168.2.4
Nov 18, 2020 22:04:25.352948904 CET	49748	4782	192.168.2.4	185.244.26.221

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 22:02:26.615756035 CET	51726	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:02:26.642864943 CET	53	51726	8.8.8.8	192.168.2.4
Nov 18, 2020 22:02:29.198508024 CET	56794	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:02:29.225600004 CET	53	56794	8.8.8.8	192.168.2.4
Nov 18, 2020 22:02:30.225917101 CET	56534	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:02:30.261406898 CET	53	56534	8.8.8.8	192.168.2.4
Nov 18, 2020 22:02:33.435633898 CET	56627	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:02:33.462861061 CET	53	56627	8.8.8.8	192.168.2.4
Nov 18, 2020 22:02:34.557153940 CET	56621	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:02:34.584332943 CET	53	56621	8.8.8.8	192.168.2.4
Nov 18, 2020 22:02:35.602444887 CET	63116	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:02:35.629566908 CET	53	63116	8.8.8.8	192.168.2.4

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 22:02:36.399518967 CET	64078	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:02:36.426800013 CET	53	64078	8.8.8.8	192.168.2.4
Nov 18, 2020 22:02:37.204504013 CET	64801	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:02:37.240169048 CET	53	64801	8.8.8.8	192.168.2.4
Nov 18, 2020 22:02:38.009109020 CET	61721	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:02:38.036233902 CET	53	61721	8.8.8.8	192.168.2.4
Nov 18, 2020 22:02:38.843467951 CET	51255	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:02:38.878778934 CET	53	51255	8.8.8.8	192.168.2.4
Nov 18, 2020 22:02:39.664978981 CET	61522	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:02:39.692018032 CET	53	61522	8.8.8.8	192.168.2.4
Nov 18, 2020 22:02:40.470731020 CET	52337	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:02:40.506336927 CET	53	52337	8.8.8.8	192.168.2.4
Nov 18, 2020 22:02:54.412713051 CET	55046	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:02:54.439892054 CET	53	55046	8.8.8.8	192.168.2.4
Nov 18, 2020 22:03:06.440885067 CET	49612	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:03:06.468094110 CET	53	49612	8.8.8.8	192.168.2.4
Nov 18, 2020 22:03:07.297065020 CET	49285	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:03:07.497384071 CET	53	49285	8.8.8.8	192.168.2.4
Nov 18, 2020 22:03:15.046999931 CET	50601	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:03:15.098958015 CET	53	50601	8.8.8.8	192.168.2.4
Nov 18, 2020 22:03:15.633944988 CET	60875	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:03:15.669302940 CET	53	60875	8.8.8.8	192.168.2.4
Nov 18, 2020 22:03:16.098850965 CET	56448	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:03:16.134459019 CET	53	56448	8.8.8.8	192.168.2.4
Nov 18, 2020 22:03:16.446012974 CET	59172	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:03:16.481395960 CET	53	59172	8.8.8.8	192.168.2.4
Nov 18, 2020 22:03:16.733311892 CET	62420	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:03:16.768939018 CET	53	62420	8.8.8.8	192.168.2.4
Nov 18, 2020 22:03:16.834768057 CET	60579	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:03:16.870117903 CET	53	60579	8.8.8.8	192.168.2.4
Nov 18, 2020 22:03:16.945837021 CET	50183	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:03:16.972923994 CET	53	50183	8.8.8.8	192.168.2.4
Nov 18, 2020 22:03:17.264987946 CET	61531	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:03:17.292031050 CET	53	61531	8.8.8.8	192.168.2.4
Nov 18, 2020 22:03:17.715737104 CET	49228	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:03:17.751249075 CET	53	49228	8.8.8.8	192.168.2.4
Nov 18, 2020 22:03:18.289900064 CET	59794	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:03:18.325318098 CET	53	59794	8.8.8.8	192.168.2.4
Nov 18, 2020 22:03:18.922276020 CET	55916	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:03:18.960123062 CET	53	55916	8.8.8.8	192.168.2.4
Nov 18, 2020 22:03:19.415637016 CET	52752	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:03:19.451225996 CET	53	52752	8.8.8.8	192.168.2.4
Nov 18, 2020 22:03:30.517765045 CET	60542	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:03:30.555037975 CET	53	60542	8.8.8.8	192.168.2.4
Nov 18, 2020 22:04:01.499881983 CET	60689	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:04:01.527025938 CET	53	60689	8.8.8.8	192.168.2.4
Nov 18, 2020 22:04:03.307820082 CET	64206	53	192.168.2.4	8.8.8.8
Nov 18, 2020 22:04:03.345563889 CET	53	64206	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 18, 2020 22:03:06.440885067 CET	192.168.2.4	8.8.8.8	0x3cb3	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)
Nov 18, 2020 22:03:07.297065020 CET	192.168.2.4	8.8.8.8	0x6a02	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 22:03:06.468094110 CET	8.8.8.8	192.168.2.4	0x3cb3	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)
Nov 18, 2020 22:03:07.497384071 CET	8.8.8.8	192.168.2.4	0x6a02	No error (0)	devils.shacknet.us		185.244.26.221	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ip-api.com

HTTP Packets

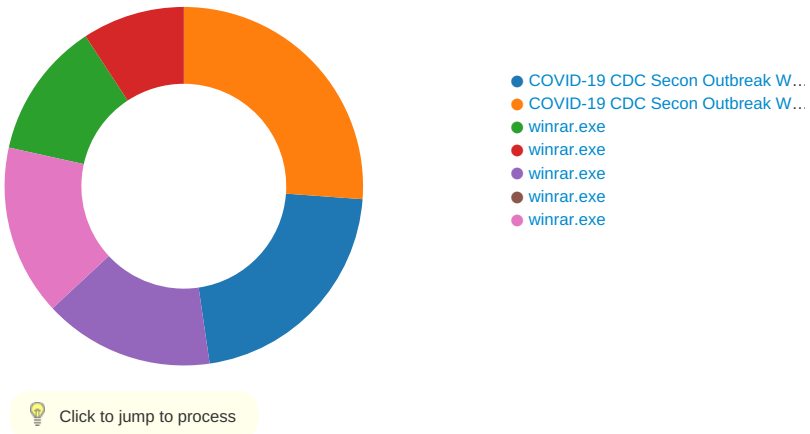
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49747	208.95.112.1	80	C:\Users\user\Desktop\COVID-19 CDC Secon Outbreak Warning release.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 22:03:06.519504070 CET	360	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 22:03:06.609174013 CET	361	IN	HTTP/1.1 200 OK Date: Wed, 18 Nov 2020 21:03:06 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: COVID-19 CDC Secon Outbreak Warning release.exe PID: 5856
Parent PID: 5964

General

Start time:	22:02:31
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\COVID-19 CDC Secon Outbreak Warning release.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\COVID-19 CDC Secon Outbreak Warning release.exe'
Imagebase:	0x6f0000
File size:	634176 bytes
MD5 hash:	DB0D632B83738DFC64013B9B5B7C339E
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: 00000000.00000002.730551537.0000000003C35000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000000.00000002.730551537.0000000003C35000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C0EBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.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	58329B3	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	58329B3	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\COVID-19 CDC Secon Outbreak Warning release.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D5AC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright null 2020

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 61 5b b3 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 42 08 00 00 38 01 00 00 00 00 00 3a 60 08 00 00 20 00 00 00 80 08 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 e0 09 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...a[._.......... ....B...8......:`... ....@.. ....@................	success or wait	3	58329B3	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.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	58329B3	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\COVID-19 CDC Secon 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\NativeIma ges_v4.0.30319_32\System\4f0a7 eefa3cd3e0ba98b5ebddbbc72e6\Sy stem.ni.dll",0..3,"System.Core, Version=4.0.0	success or wait	1	6D5AC907	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	6D275705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D275705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D27CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1D03DE	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	winrar	unicode	"C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe"	success or wait	1	6C0E646A	RegSetValueExW

Analysis Process: COVID-19 CDC Secon Outbreak Warning release.exe PID: 7040 Parent PID: 5856

General

Start time:	22:03:01
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\COVID-19 CDC Secon Outbreak Warning release.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\COVID-19 CDC Secon Outbreak Warning release.exe
Imagebase:	0xf80000
File size:	634176 bytes
MD5 hash:	DB0D632B83738DFC64013B9B5B7C339E
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: 00000003.00000002.924590953.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000003.00000002.924590953.0000000000402000.00000040.00000001.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	6D29CF06	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	6D29CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\COVID-19 CDC Secon Outbreak Warning release.exe:Zone.Identifier	success or wait	1	58674CA	DeleteFileW

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	6D275705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D275705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D27CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D27CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D275705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D275705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D1D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C0E1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: winrar.exe PID: 6972 Parent PID: 3424

General

Start time:	22:03:07
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe'
Imagebase:	0xc70000
File size:	634176 bytes
MD5 hash:	DB0D632B83738DFC64013B9B5B7C339E
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: 00000005.00000002.808237163.00000000042C5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000005.00000002.808237163.00000000042C5000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 53%, Virustotal, Browse • Detection: 14%, Metadefender, Browse • Detection: 59%, ReversingLabs
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\Local\Microsoft\CLR_v4.0_32\UsageLogs\winrar.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D5AC78D	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\winrar.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	6D5AC907	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	6D275705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D275705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D27CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1D03DE	ReadFile

Analysis Process: winrar.exe PID: 4576 Parent PID: 3424

General

Start time:	22:03:15
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe'
Imagebase:	0xbe0000
File size:	634176 bytes
MD5 hash:	DB0D632B83738DFC64013B9B5B7C339E
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: 00000009.00000002.822302365.00000000040E1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000009.00000002.822302365.00000000040E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000009.00000002.822958398.00000000041C5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000009.00000002.822958398.00000000041C5000.00000004.00000001.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	6D275705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D275705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D27CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1D03DE	ReadFile

Analysis Process: winrar.exe PID: 5256 Parent PID: 6972

General

Start time:	22:03:37
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe
Imagebase:	0xb20000
File size:	634176 bytes
MD5 hash:	DB0D632B83738DFC64013B9B5B7C339E
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: 0000000D.00000002.808322166.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 0000000D.00000002.808322166.0000000000402000.00000040.00000001.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	6D29CF06	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	6D29CF06	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	6D275705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D275705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D27CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D275705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D275705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1D03DE	ReadFile

Analysis Process: winrar.exe PID: 5572 Parent PID: 4576

General

Start time:	22:03:46
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe
Imagebase:	0xb0000
File size:	634176 bytes
MD5 hash:	DB0D632B83738DFC64013B9B5B7C339E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: winrar.exe PID: 5576 Parent PID: 4576

General

Start time:	22:03:46
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Winrar\winrar.exe
Imagebase:	0x710000
File size:	634176 bytes
MD5 hash:	DB0D632B83738DFC64013B9B5B7C339E
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.00000002.827897659.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 0000000F.00000002.827897659.0000000000402000.00000040.00000001.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	6D29CF06	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	6D29CF06	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	6D275705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D275705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D27CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D275705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D275705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1D03DE	ReadFile

Disassembly

Code Analysis

Copyright null 2020