ID: 397590
Sample Name: COVID 19 BENEFIT FORM 2.exe
Cookbook: default.jbs
Time: 08:10:52
Date: 26/04/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

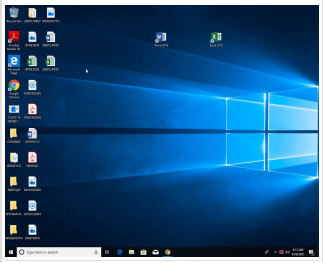
Analysis Report COVID 19 BENEFIT FORM 2.exe

Overview

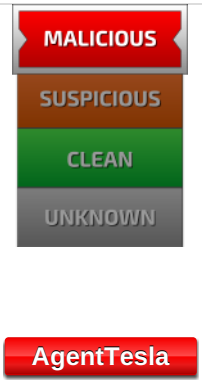
General Information

Sample Name:	COVID 19 BENEFIT FORM 2.exe
Analysis ID:	397590
MD5:	734dcc6ee873ad..
SHA1:	205b63e53d5789..
SHA256:	cce12e2162f90a8..
Tags:	AgentTesla COVID-19 exe
Infos:	

Most interesting Screenshot:



Detection



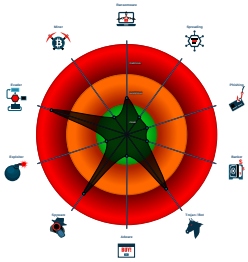
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…

Classification



Startup

- **System is w10x64**
- COVID 19 BENEFIT FORM 2.exe (PID: 6424 cmdline: 'C:\Users\user\Desktop\COVID 19 BENEFIT FORM 2.exe' MD5: 734DCC6EE873AD6667D9CAD4E5040134)
  - schtasks.exe (PID: 6880 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lVGkcjmu' /XML 'C:\Users\user\AppData\Local\Temp\tmp764A.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - COVID 19 BENEFIT FORM 2.exe (PID: 6976 cmdline: {path} MD5: 734DCC6EE873AD6667D9CAD4E5040134)
  - COVID 19 BENEFIT FORM 2.exe (PID: 6984 cmdline: {path} MD5: 734DCC6EE873AD6667D9CAD4E5040134)
  - COVID 19 BENEFIT FORM 2.exe (PID: 6992 cmdline: {path} MD5: 734DCC6EE873AD6667D9CAD4E5040134)
  - COVID 19 BENEFIT FORM 2.exe (PID: 7000 cmdline: {path} MD5: 734DCC6EE873AD6667D9CAD4E5040134)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "logs@seedchangeinv.commmm777@@mail.privateemail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.596294759.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000A.00000002.599311455.000000000281000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000A.00000002.599311455.000000000281000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
00000000.00000002.377564391.00000000040CD000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.377324089.0000000003F29000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 4 entries				

Unpacked PEs

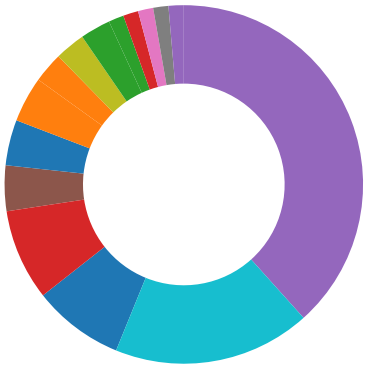
Source	Rule	Description	Author	Strings
0.2.COVID 19 BENEFIT FORM 2.exe.4293c80.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
10.2.COVID 19 BENEFIT FORM 2.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.COVID 19 BENEFIT FORM 2.exe.4293c80.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Boot Survival:

Copyright Joe Security LLC 2021

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, 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:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

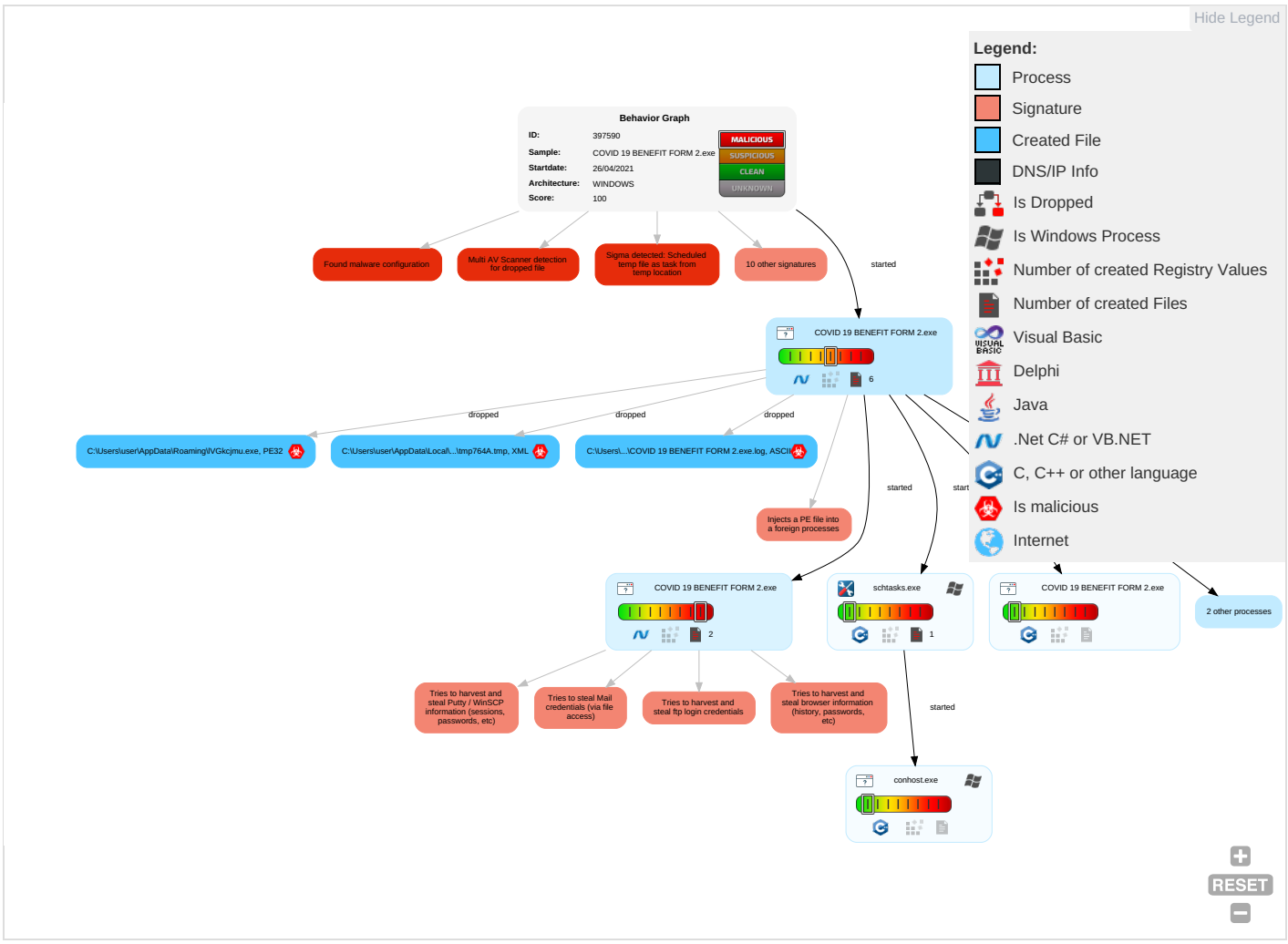
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	Credentials in Registry 1	Security Software Discovery 3 2 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 4 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Steganograph
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 4 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Protocol Impersonatio
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

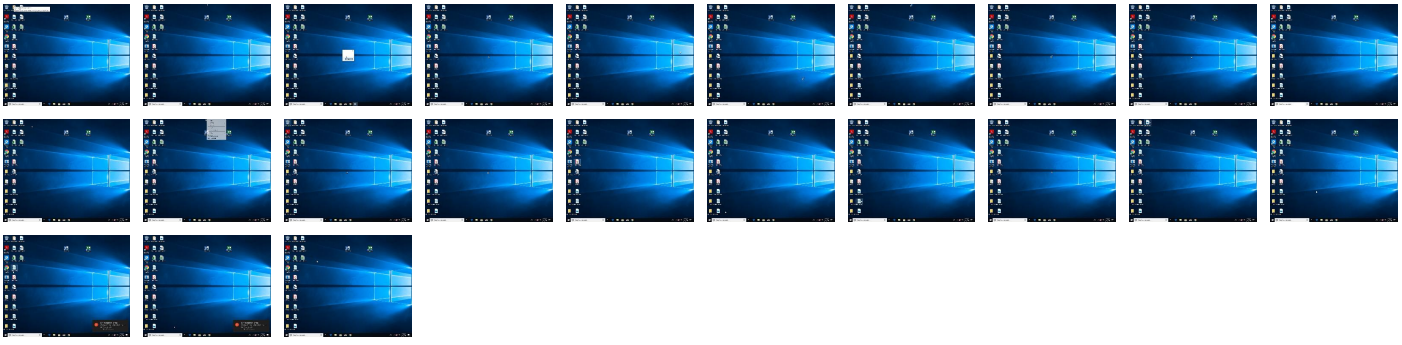
Behavior Graph



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 BENEFIT FORM 2.exe	43%	Virustotal		Browse
COVID 19 BENEFIT FORM 2.exe	37%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
COVID 19 BENEFIT FORM 2.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\lVGkcjmu.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\lVGkcjmu.exe	37%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.COVID 19 BENEFIT FORM 2.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.htmlnW/	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr-c	0%	Avira URL Cloud	safe	
http://www.tiro.comn-u3	0%	Avira URL Cloud	safe	
http://www.urwpp.deWE0	0%	Avira URL Cloud	safe	
http://www.carterandcone.comen	0%	URL Reputation	safe	
http://www.carterandcone.comen	0%	URL Reputation	safe	
http://www.carterandcone.comen	0%	URL Reputation	safe	
http://www.carterandcone.comWF3	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krn-usur	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnr-f	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.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.fontbureau.comgreta	0%	URL Reputation	safe	
http://www.fontbureau.comgreta	0%	URL Reputation	safe	
http://www.fontbureau.comgreta	0%	URL Reputation	safe	
http://www.goodfont.co.krx.	0%	Avira URL Cloud	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.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	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.tiro.comWE0	0%	Avira URL Cloud	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.carterandcone.comtig	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.sandoll.co.krq	0%	Avira URL Cloud	safe	
http://www.urwpp.deLE;	0%	Avira URL Cloud	safe	
http://www.carterandcone.comNF8	0%	Avira URL Cloud	safe	
http://www.carterandcone.compt	0%	Avira URL Cloud	safe	
http://www.urwpp.deiEEB	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.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.zhongyicts.com.cna	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr)Rr	0%	Avira URL Cloud	safe	
http://www.carterandcone.comx	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnK	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnK	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://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://www.urwpp.deEEB	0%	Avira URL Cloud	safe	
http://www.carterandcone.com0	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn;	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/FqR	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.comJhEB	0%	Avira URL Cloud	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.fontbureau.comiona	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	COVID 19 BENEFIT FORM 2.exe, 0000000A.00000002.599311455.0000002871000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.ascendercorp.com/typedesigners.htmlnW/	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.334231166.0000005EA3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr-c	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.331486082.0000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.comn-u3	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332246844.00000015EC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deWE0	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.339197866.0000005EA8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comen	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.333039942.0000005E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000005F70000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comWF3	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.333039942.0000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krn-usur	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.331486082.0000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnr-f	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332430336.0000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000005F70000.00000002.00000001.sdmp, COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.328572795.0000000005E82000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers-Sq	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.337167523.0000005E9B000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000005F70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comgreta	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.375338319.00000015E7000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.krx.	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.331486082.0000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000005F70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.334907624.0000005EA3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000005F70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332725617.0000005E9B000.00000004.00000001.sdmp, COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000000005F70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comWE0	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.333146895.0000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.375417166.0000002F21000.00000004.00000001.sdmp	false		high
http://www.carterandcone.como.	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332725617.0000005E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org%	COVID 19 BENEFIT FORM 2.exe, 0000000A.00000002.599311455.0000000002871000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.377324089.0000000003F29000.00000004.00000001.sdmp, COVID 19 BENEFIT FORM 2.exe, 0000000A.00000002.596294759.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comtig	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332725617.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	COVID 19 BENEFIT FORM 2.exe, 0000000A.00000002.601224082.0000000002BD1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.come	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332725617.0000000005E9B000.00000004.00000001.sdmp, COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332479184.0000000005E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.htmlf	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.337387930.0000000005E9B000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersES	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.345153128.0000000005E9B000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	COVID 19 BENEFIT FORM 2.exe, 0000000A.00000002.599311455.0000000002871000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krq	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.331540177.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deLE;	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.336364737.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.comNF8	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.333039942.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.compt	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.333146895.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deiEEB	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.336364737.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.privateemail.com	COVID 19 BENEFIT FORM 2.exe, 0000000A.00000002.601224082.0000000002BD1000.00000004.00000001.sdmp	false		high
http://en.w	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.330293022.0000000005EAA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000000005F70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332128006.0000000005E9B000.00000004.00000001.sdmp, COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.331974163.0000000005EA2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.337413588.0000000005EBE000.00000004.00000001.sdmp, COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000000005F70000.00000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cna	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332725617.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr)Rr	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.331486082.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.comx	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.333146895.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnK	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332725617.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000000005F70000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersF	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.337167523.0000000005E9B000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnK	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332128006.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000000005F70000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000000005F70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	COVID 19 BENEFIT FORM 2.exe, 000000A.00000002.601224082.0000002BD1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000000005F70000.00000002.00000001.sdmp	false		high
http://www.urwpp.deEEB	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.338840406.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersB	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.345153128.0000000005E9B000.00000004.00000001.sdmp	false		high
http://www.carterandcone.com0	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332725617.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000000005F70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn;	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332725617.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/FqR	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.331540177.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000000005F70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332725617.0000000005E9B000.00000004.00000001.sdmp, COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332816319.0000000005E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comJhEB	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.333039942.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comiona	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.375338319.00000015E7000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000005F70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.341196577.0000000005E9B000.00000004.00000001.sdmp, COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000000005F70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.329792577.0000000005E9B000.00000004.00000001.sdmp, COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000000005F70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnk	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332128006.0000005E9B000.00000004.00000001.sdmp	false		unknown
http://www.founder.com.cn/cnl	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332128006.0000005E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.k	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.331540177.0000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	COVID 19 BENEFIT FORM 2.exe, 000000A.00000002.599311455.0000002871000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000005F70000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.331486082.0000005E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comTC(Sr	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332725617.0000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.comac	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.333146895.0000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.336364737.0000005E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000005F70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comic	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.333039942.0000005E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comn	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.328572795.0000005E82000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.come5BV	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.333146895.0000000E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000005F70000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.375338319.00000015E7000.00000004.00000040.sdmp	false		high
http://DynDns.comDynDNS	COVID 19 BENEFIT FORM 2.exe, 000000A.00000002.599311455.0000002871000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	COVID 19 BENEFIT FORM 2.exe, 000000A.00000002.601224082.0000002BD1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mapoex.com	COVID 19 BENEFIT FORM 2.exe, 000000A.00000002.599311455.0000002871000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://SBRGHbI6v8zShNk.netL2	COVID 19 BENEFIT FORM 2.exe, 000000A.00000002.599311455.0000002871000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTC	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332816319.0000005E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://SBRGHbI6v8zShNk.net	COVID 19 BENEFIT FORM 2.exe, 000000A.00000002.599311455.0000002871000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comlt	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332725617.0000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/typedesigners.htmlBW	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.334907624.0000005EA3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmld	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.338045037.0000005EBE000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlh	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.338606084.0000005EBE000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000005F70000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.331820934.0000005EA4000.00000004.00000001.sdmp, COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.331864305.0000000005EA0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.kra-es)Rr	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.331382313.0000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.monotype.)Qr	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.336815155.0000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.monotype.	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.341196577.0000005E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000005F70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers#	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.338116776.0000000005E9B000.00000004.00000001.sdmp	false		high
http://www.zhongyicts.com.cno.	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332430336.0000000005E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	COVID 19 BENEFIT FORM 2.exe, 00000000.00000002.382360322.0000000005F70000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersdSF	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.338116776.0000000005E9B000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnof	COVID 19 BENEFIT FORM 2.exe, 00000000.00000003.332128006.0000000005E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	397590
Start date:	26.04.2021
Start time:	08:10:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	COVID 19 BENEFIT FORM 2.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:	27
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.spyw.evad.winEXE@12/3@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.9% (good quality ratio 0.8%) • Quality average: 74.6% • Quality standard deviation: 36.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:11:53	API Interceptor	604x Sleep call for process: COVID 19 BENEFIT FORM 2.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\COVID 19 BENEFIT FORM 2.exe.log

Process:	C:\Users\user\Desktop\COVID 19 BENEFIT FORM 2.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\COVID 19 BENEFIT FORM 2.exe.log	
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp764A.tmp	
Process:	C:\Users\user\Desktop\COVID 19 BENEFIT FORM 2.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1653
Entropy (8bit):	5.161424567837416
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3gtn:cbha7JlNQV/rydbz9l3YODOLNdq3w
MD5:	16A94BE6EBAD3568D9448D68732242F7
SHA1:	469EA4CEFC16BB192AB7B77402726772270AF094
SHA-256:	8AF2CDA081DBA7360EB8167F9838F5E768748461125E9E22F35B6FFD6088EE34
SHA-512:	09DC435C8D28F0C7785AD1A4D8E0399DF68DF84D5A6C61B208449D88B40189156527CAF42CF55CD0C69206A3BC37570AB30177B8812BFFB192C62A040FD46C4
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\IVGkcjmu.exe	
Process:	C:\Users\user\Desktop\COVID 19 BENEFIT FORM 2.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1059328
Entropy (8bit):	7.553054120628421
Encrypted:	false
SSDEEP:	24576:sCoLASBuls9O+ITcyZwBCrKaPW1P6GT4g6T98UAKL4M:22s9OjAyuBQNP6p6T6ZE
MD5:	734DCC6EE873AD6667D9CAD4E5040134
SHA1:	205B63E53D5789F469BDFAFDFB553E74B967F5DF
SHA-256:	CCE12E2162F90A88715E50BFA993E9D3233FECAF608FB18CDA68F0154F0E1D5B
SHA-512:	61B9DD380EFFC682868EE45D7C1A789A6F516409586F93908A3CBC222300AFAA8BC309719E68A63DD0C2095955138C9F75B041DBD0B234FF824D21C8949E7EA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 37%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...$&.....0.. .....?... ...@....@.. .....@.....?..O....@.....`.....d?..... ..... ..H.....text..... ... ..... ..`.rsrc.....@.....".....@..@.reloc.....`.....(.....@..B.....?.....H.....$....e.....s.....pE.....".(....*V.(.....(....}....*..0..!.....{....o....o....o....o....+..*....0..M.....{....o....o....o....o....o....o....r...po.....{....o ....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*..{....*^.(.....}.....}....*....0.....r/..p.+..*..0.....rY..p.+..*".(....*2.{....o'...*2.{....o(...*..{....*"..}....*..{....*"..}....*..{....*"..}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.553054120628421

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	COVID 19 BENEFIT FORM 2.exe
File size:	1059328
MD5:	734dcc6ee873ad6667d9cad4e5040134
SHA1:	205b63e53d5789f469bdfafdfb553e74b967f5df
SHA256:	cce12e2162f90a88715e50bfa993e9d3233fecaf608fb18cda68f0154f0e1d5b
SHA512:	61b9dd380effc682868ee45d7c1a789a6f516409586f93908a3cbc222300afaa8bc309719e68a63dd0c2095955138c9f75b041dbd0b234ff824d21c8949e7ea5
SSDEEP:	24576:sCoLASBuls9O+ITcyZwBCrKaPW1P6GT4g6T98UAKL4M:22s9OjAyuBQNP6p6T6ZE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...$&.....0.. .....?... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x503fd2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xD4A32624 [Mon Jan 18 01:38:44 2083 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Copyright Joe Security LLC 2021

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 al, byte ptr [eax]
adc byte ptr [eax], al
add byte ptr [eax], al
and byte ptr [eax], al
add byte ptr [eax+00000018h], al
push eax
add byte ptr [eax], al
add byte ptr [eax], 00000000h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add dword ptr [eax], eax
add byte ptr [eax], al
cmp byte ptr [eax], al
add byte ptr [eax+00000000h], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], 00000000h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax+00h], ch
add byte ptr [eax+00000000h], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
les eax, fword ptr [ebx]

Instruction
add byte ptr [eax], al
nop
inc eax
adc byte ptr [eax], al
xor al, 03h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor al, 03h
xor al, 00h
add byte ptr [eax], al
push esi
add byte ptr [ebx+00h], dl

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x103f80	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x104000	0x5c4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x106000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x103f64	0x1c	.text
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	0x101fd8	0x102000	False	0.79585396227	data	7.55509346108	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x104000	0x5c4	0x600	False	0.4296875	data	4.19069643928	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x106000	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_VERSION	0x104090	0x334	data		
RT_MANIFEST	0x1043d4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020
Assembly Version	1.0.0.0
InternalName	3Y6kOc.exe

Description	Data
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	POSCashSystem
ProductVersion	1.0.0.0
FileDescription	POSCashSystem
OriginalFilename	3Y6kOc.exe

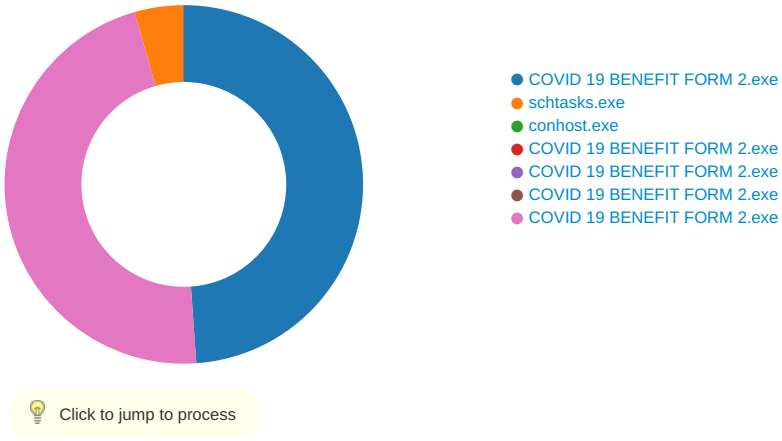
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: COVID 19 BENEFIT FORM 2.exe PID: 6424 Parent PID: 5872

General

Start time:	08:11:41
Start date:	26/04/2021
Path:	C:\Users\user\Desktop\COVID 19 BENEFIT FORM 2.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\COVID 19 BENEFIT FORM 2.exe'
Imagebase:	0xb60000
File size:	1059328 bytes
MD5 hash:	734DCC6EE873AD6667D9CAD4E5040134
Has elevated privileges:	true

Copyright Joe Security LLC 2021

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.377564391.00000000040CD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.377324089.0000000003F29000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DE8CF06	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	6DE8CF06	unknown
C:\Users\user\AppData\Roaming\IVGkcjmu.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CCD1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp764A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CCD7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\COVID 19 BENEFIT FORM 2.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E19C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp764A.tmp	success or wait	1	6CCD6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\lVGkcjmu.exe	unknown	1059328	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 24 26 a3 d4 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 20 10 00 00 08 00 00 00 00 00 00 d2 3f 10 00 00 20 00 00 00 40 10 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 10 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.... $.......PE..L...$&............ ....0.. ....?... ...@....@.. ....@................	success or wait	1	6CCD1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp764A.tmp	unknown	1653	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </Registratio	success or wait	1	6CCD1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\COVID 19 BENEFIT FORM 2.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E19C907	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	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE6CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCD1B4F	ReadFile
C:\Users\user\Desktop\COVID 19 BENEFIT FORM 2.exe	unknown	1059328	success or wait	1	6CCD1B4F	ReadFile

Analysis Process: schtasks.exe PID: 6880 Parent PID: 6424

General

Start time:	08:12:00
Start date:	26/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\IVGkcjmu' /XML 'C:\Users\user\AppData\Local\Temp\tmp764A.tmp'
Imagebase:	0x1210000
File size:	185856 bytes

MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp764A.tmp	unknown	2	success or wait	1	121AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp764A.tmp	unknown	1654	success or wait	1	121ABD9	ReadFile

Analysis Process: conhost.exe PID: 6936 Parent PID: 6880

General

Start time:	08:12:01
Start date:	26/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: COVID 19 BENEFIT FORM 2.exe PID: 6976 Parent PID: 6424

General

Start time:	08:12:01
Start date:	26/04/2021
Path:	C:\Users\user\Desktop\COVID 19 BENEFIT FORM 2.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x2a0000
File size:	1059328 bytes
MD5 hash:	734DCC6EE873AD6667D9CAD4E5040134
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: COVID 19 BENEFIT FORM 2.exe PID: 6984 Parent PID: 6424

General

Start time:	08:12:02
Start date:	26/04/2021
Path:	C:\Users\user\Desktop\COVID 19 BENEFIT FORM 2.exe

Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x60000
File size:	1059328 bytes
MD5 hash:	734DCC6EE873AD6667D9CAD4E5040134
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: COVID 19 BENEFIT FORM 2.exe PID: 6992 Parent PID: 6424

General

Start time:	08:12:02
Start date:	26/04/2021
Path:	C:\Users\user\Desktop\COVID 19 BENEFIT FORM 2.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x220000
File size:	1059328 bytes
MD5 hash:	734DCC6EE873AD6667D9CAD4E5040134
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: COVID 19 BENEFIT FORM 2.exe PID: 7000 Parent PID: 6424

General

Start time:	08:12:03
Start date:	26/04/2021
Path:	C:\Users\user\Desktop\COVID 19 BENEFIT FORM 2.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x4c0000
File size:	1059328 bytes
MD5 hash:	734DCC6EE873AD6667D9CAD4E5040134
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.596294759.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.599311455.0000000002871000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.599311455.0000000002871000.00000004.00000001.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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DE8CF06	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	6DE8CF06	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	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE6CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCD1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CCD1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CCD1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CCD1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6CCD1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\11a1f504-ab5d-4e2b-99f1-1af390edf3b6	unknown	4096	success or wait	1	6CCD1B4F	ReadFile

Disassembly

Code Analysis

Copyright Joe Security LLC 2021