ID: 468641
Sample Name: Covid narrative 6.20 8.21 to bank.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 06:28:16
Date: 20/08/2021
Version: 33.0.0 White Diamond

Table of Contents

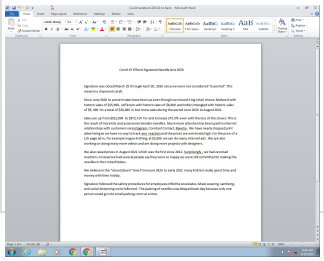
Windows Analysis Report Covid narrative 6.20 8.21 to b…

Overview

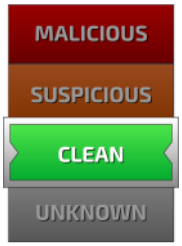
General Information

Sample Name:	Covid narrative 6.20 8.21 to bank.docx
Analysis ID:	468641
MD5:	2474cd82664b91..
SHA1:	6360310aa9f9a8a.
SHA256:	b77efefb8a22a24..
Tags:	doc docx
Infos:	

Most interesting Screenshot:



Detection

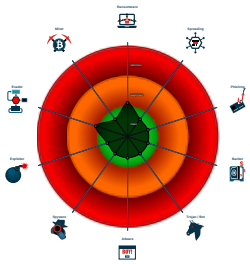


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2724 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

Jbx Signature Overview

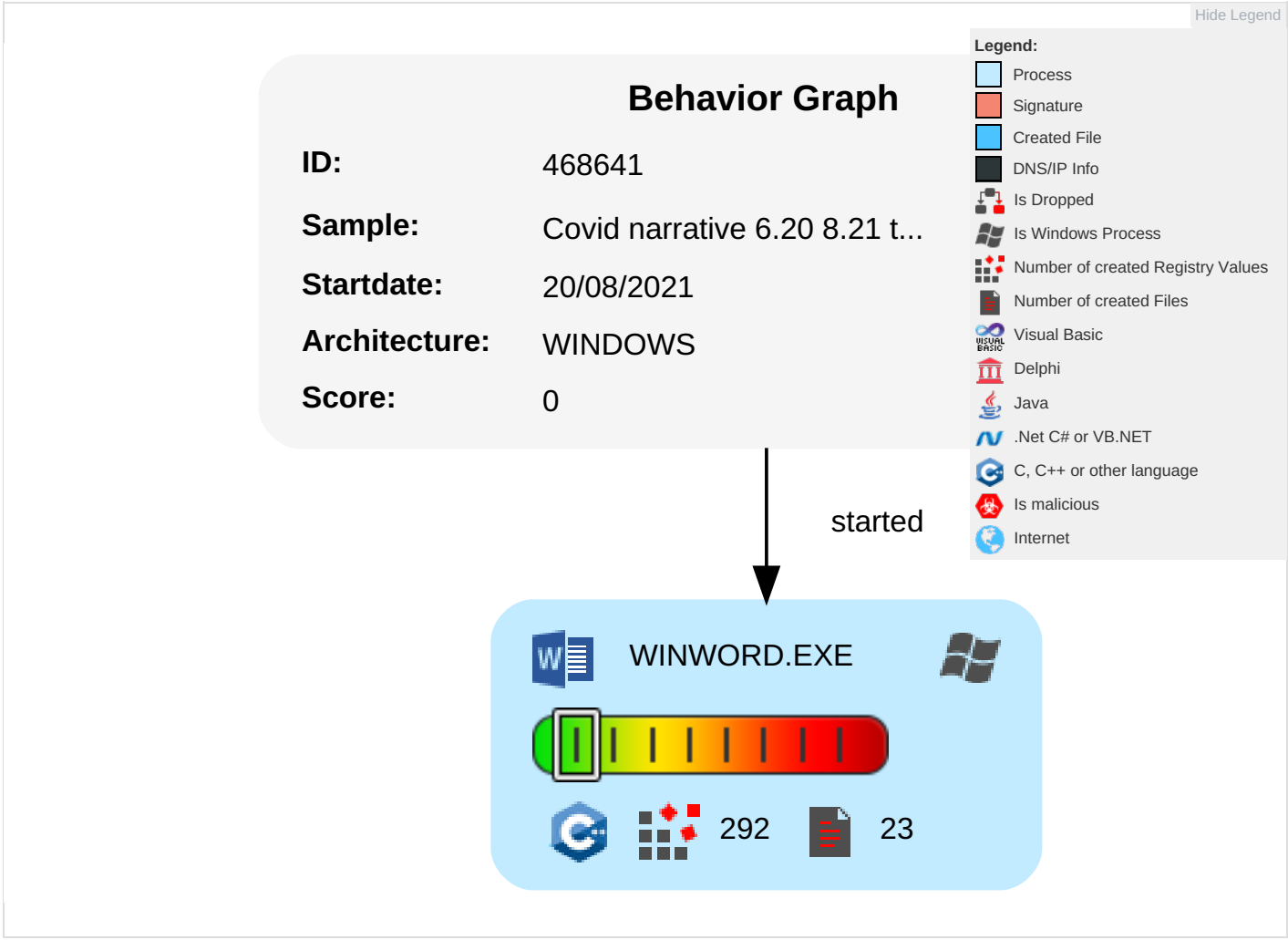
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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	Impact
Valid Accounts	Windows Management Instrumentation	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	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	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	Device Lockout

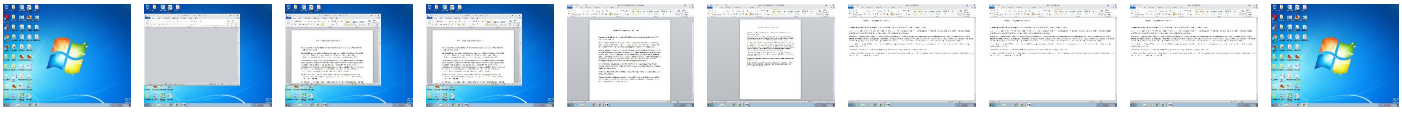
Behavior Graph

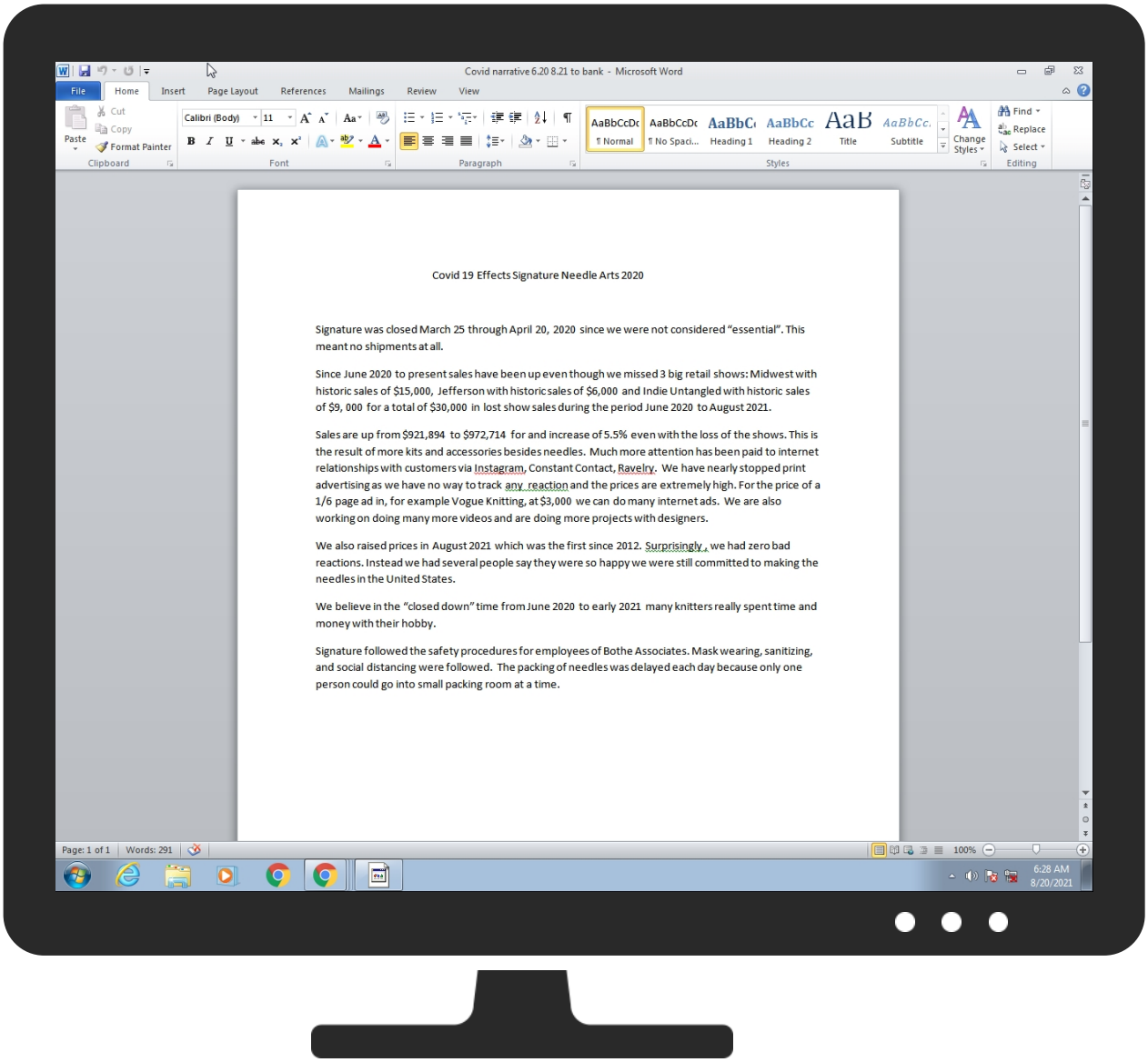


Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

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

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	468641
Start date:	20.08.2021
Start time:	06:28:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Covid narrative 6.20 8.21 to bank.docx
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winDOCX@1/7@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

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.Word\~WRS{03EBD8D7-10B9-4A25-A35B-CDE7E003844A}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	4394
Entropy (8bit):	2.8996504281778237
Encrypted:	false
SSDEEP:	96:Yla+V5/yGrpjG0EuzXUzEQQxlg0hWbktkE:P+bTjG0zXjxrA4aE
MD5:	3B1BE8F00443847F58CD56935C7CA436
SHA1:	65E6E79C49B9E298946D2E8E5EDDA33128D69478
SHA-256:	357821DA72272EDF301BF4041D48B7B671E012C22EAA8994A1302AC489BCED5C
SHA-512:	45B9EE899980163ECF4B29B9AE05FE9EDF310FF6BF7278F60D610E5818A64C52508DFA7A11AC01540BA5D8A3D6E1FE08A2327A12003C16812F8666D5069EC91E
Malicious:	false
Reputation:	low
Preview:	..C.o.v.i.d. .1.9. .E.f.f.e.c.t.s. .S.i.g.n.a.t.u.r.e. .N.e.e.d.l.e. .A.r.t.s. .2.0.2.0.....S.i.g.n.a.t.u.r.e. .w.a.s. .c.l.o.s.e.d. .M.a.r.c.h. .2.5. .t.h.r.o.u.g.h. .A.p.r.i.l. .2.0.,. .2.0.2.0. .s.i.n.c.e. .w.e. .w.e.r.e. .n.o.t. .c.o.n.s.i.d.e.r.e.d. .. e.s.s.e.n.t.i.a.l.. .. .T.h.i.s. .m.e.a.n.t. .n.o. .s.h.i.p.m.e.n.t.s. .a.t. .a.l.l... ...S.i.n.c.e. .J.u.n.e. .2.0.2.0. .t.o. .p.r.e.s.e.n.t. .s.a.l.e.s. .h.a.v.e. .b.e.e.n. .u.p. .e.v.e.n. .t.h.o.u.g.h. .w.e. .m.i.s.s.e.d. .3. .b.i.g. .r.e.t.a.i.l. .....Z...\...\.....`...2...2..... ....gd_$4.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E1A454EA-72A2-4470-89E8-B7D87A58E0E0}.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
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Covid narrative 6.20 8.21 to bank.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 14:08:14 2020, mtime=Wed Aug 26 14:08:14 2020, atime=Fri Aug 20 12:28:32 2021, length=13120, window=hide
Category:	dropped
Size (bytes):	2268
Entropy (8bit):	4.560990308141455
Encrypted:	false
SSDEEP:	48:85Q9d/XT0jF8Jx4tsQh25Q9d/XT0jF8Jx4tsQ/:8Cd/XojF8JEsQh2Cd/XojF8JEsQ/
MD5:	FC2D3B35673F7AF2E5578DC7E413353E
SHA1:	8569356EA2460FFA12129712673BB4BE5D8AE70B
SHA-256:	2766512EE6E899F1FCAD4ACC498CD04CC315F52BC599C6E005A9F57673B9C861
SHA-512:	A0020E09B3B90DB330CE1B3FBB56A32EC2B5C4B979ED6AAF80CFA7A4120D2F17CF8C4771211C58D4A092C34EA087F9B1527A114BA2D74E482B38D84CBF3253BB
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...~-z..{..~-z..{.....E...@3.....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.@3...S.k .COVIDN~1.DOC..z.....Q.y.Q.y*...8.....C.o.v.i.d. .n.a.r.r.a.t.i.v.e. .6...2.0. .8...2.1. .t.o. .b.a.n.k...d.o.c.x.....-...8...[.....?J.....C:\Users\..#.....\\284992\Users.user\Desktop\Covid narrative 6.20 8.21 to bank.docx.=....\....\....\....\....\.D.e.s.k.t.o.p.\.C.o.v.i.d. .n.a.r.r.a.t.i.v.e. .6...2.0. .8...2.1. .t.o. .b.a.n.k...d.o.c.x.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.

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):	139
Entropy (8bit):	4.683629094556507
Encrypted:	false
SSDEEP:	3:HtlwH4MTWpn8eHELkBVo+xzwH4MTWpn8eHELkBVomxWtlwH4MTWpn8eHELkBVov:HtlwYLhHiOVrzwYLhHiOVelwYLhHiOVy
MD5:	4CBE93DAA48934A5AE5641A892F9C996
SHA1:	855368738A86DF544C2D46086700E00E5FFAAD69
SHA-256:	73B2B620C1A658FD1208925194E66B3DE2A75CA3FFF1363BE884D468C2275AFD
SHA-512:	8D65592A87461D5C04D7C1008DB9C7E074DBFA9327FA23FFE76F3271D4AC56093E080D2C1F16AA64D0DC53EA441BB37069C33E8574AABA4355E7B8AE4C19008C
Malicious:	false
Reputation:	low
Preview:	[misc]..Covid narrative 6.20 8.21 to bank.LNK=0..Covid narrative 6.20 8.21 to bank.LNK=0..[misc]..Covid narrative 6.20 8.21 to bank.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:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\Desktop\~$vid narrative 6.20 8.21 to bank.docx	
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:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.230371041604221
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	Covid narrative 6.20 8.21 to bank.docx
File size:	13120
MD5:	2474cd82664b91e19e6980172f87354b
SHA1:	6360310aa9f9a8ab759ac0df1d311458d499ad4a
SHA256:	b77efefb8a22a24a9adb7ac682209f9a0b586a548008c6e b75978f4869fa439e
SHA512:	4826db406e2af4bc380b5a0024285be04d14177b5c8b90 5849c30eba7ad7eac80eba29c55b38433bccec83587298 6ae3c1c101fb75464873d0bcfd239986a79d
SSDEEP:	192:CtEvGREJ+nKFg5oCIo/lQ0reOmoWMuKFT+spo0If FxDNxpZgo7M/wC:aEvlJTi5oDMlH7RNosBIfZGo4wC
File Content Preview:	PK.....!....lZ... .....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 2724 Parent PID: 584

General

Start time:	06:28:33
Start date:	20/08/2021
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:	0x13fe90000
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

Show Windows behavior

File Created

File Deleted

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Disassembly