ID: 490191
Sample Name: Appendix 2 210823_COVID Safe Checklist for Suppliers.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 05:32:07
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

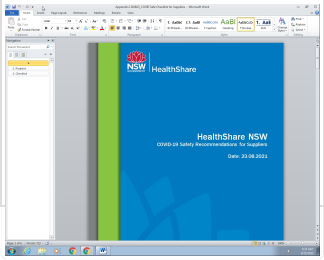
Windows Analysis Report Appendix 2 210823_COVID S…

Overview

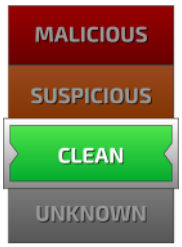
General Information

Sample Name:	Appendix 2 210823_COVID Safe Checklist for Suppliers.docx
Analysis ID:	490191
MD5:	351ca19e59770d..
SHA1:	4c688de3fe209af..
SHA256:	5a426bd44b10b1..
Infos:	

Most interesting Screenshot:



Detection

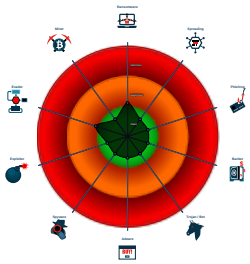


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1180 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

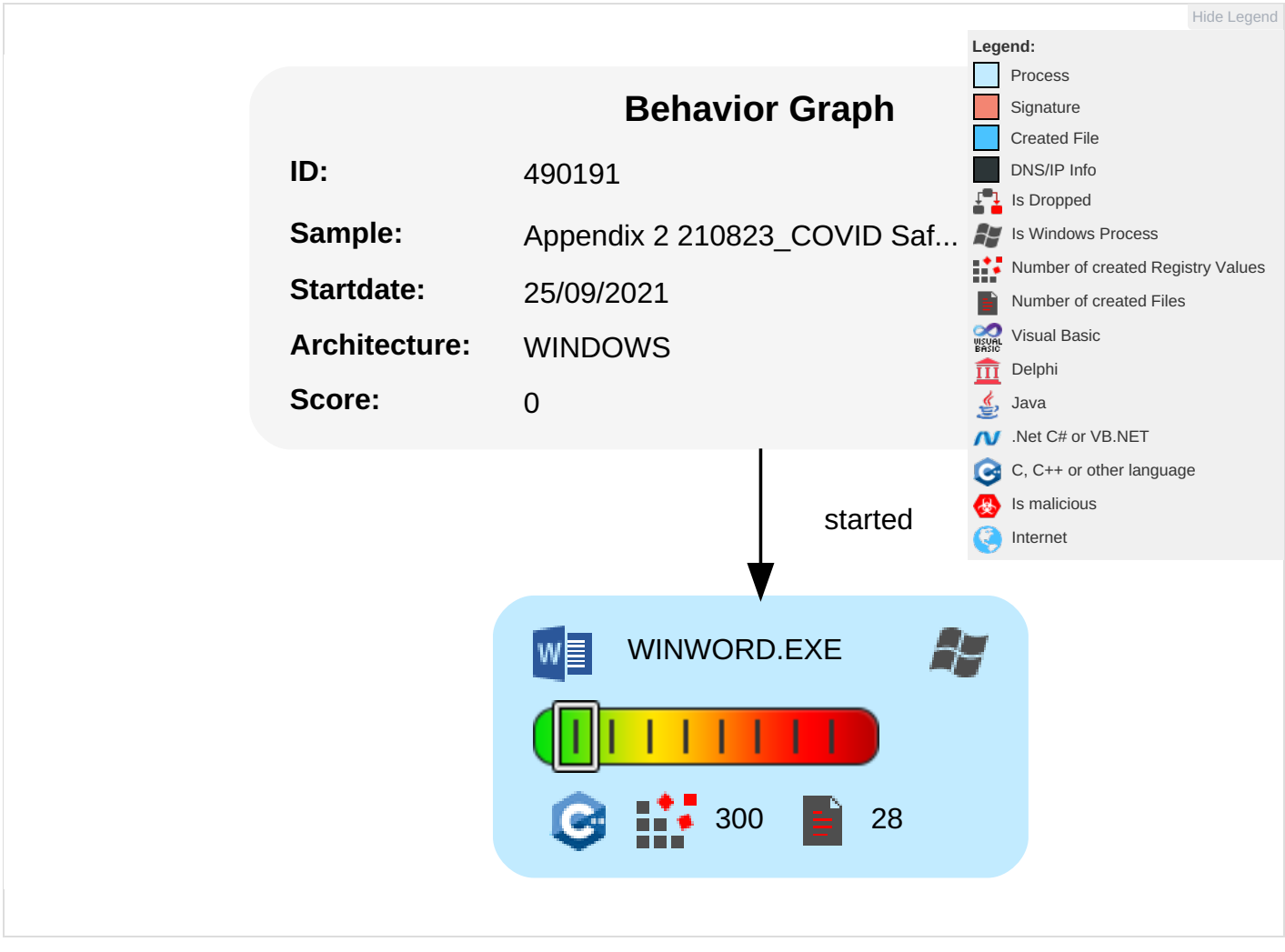
Click to jump to signature section

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

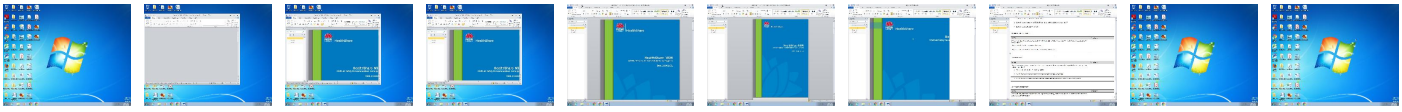
Behavior Graph

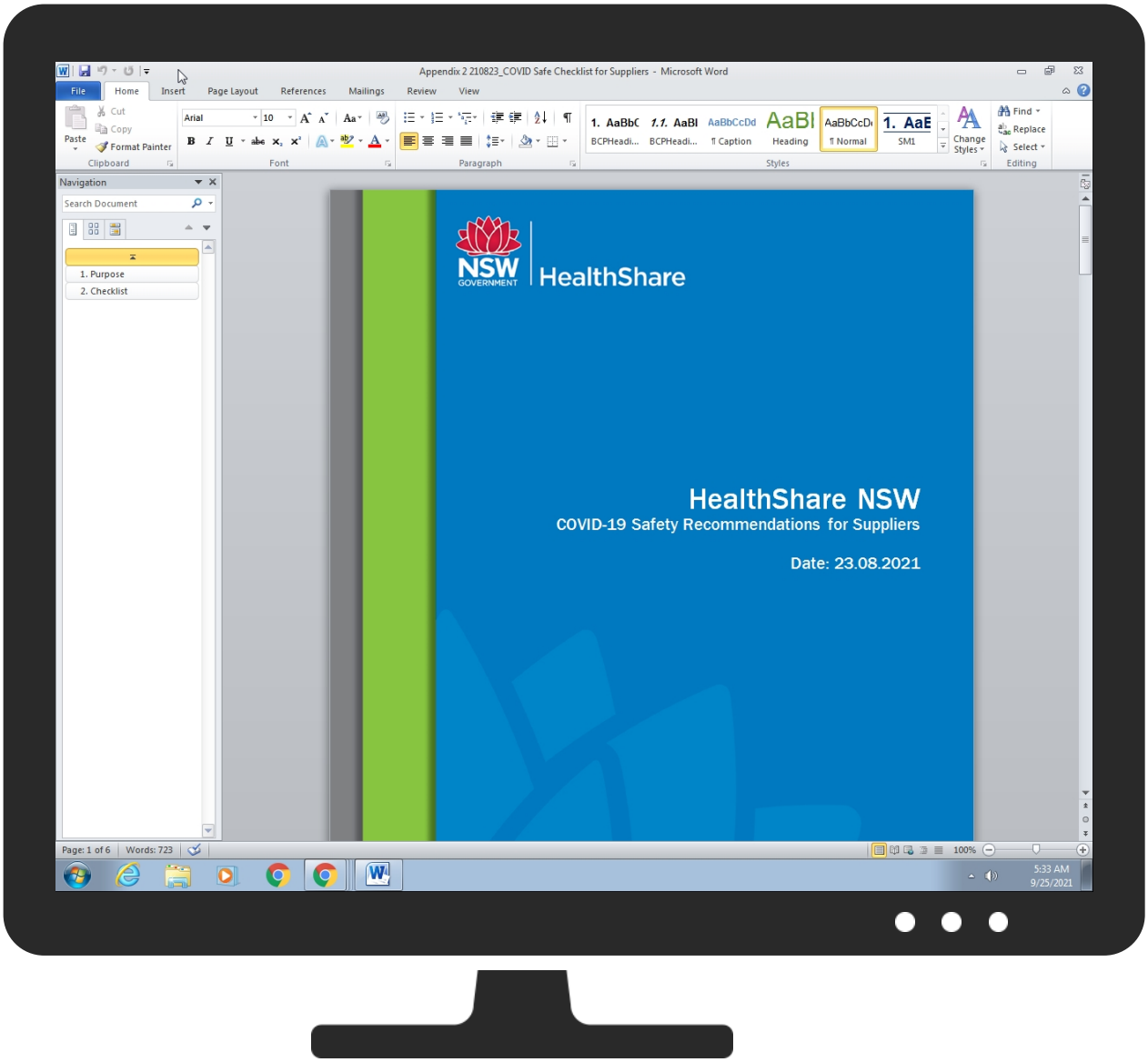


Screenshots

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:	490191
Start date:	25.09.2021
Start time:	05:32:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Appendix 2 210823_COVID Safe Checklist for Suppliers.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	3
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@1/10@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.MSO\57F34A4A.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CS5.1 Windows, datetime=2012:03:28 10:01:36], baseline, precision 8, 992x1403, frames 3
Category:	dropped
Size (bytes):	198885
Entropy (8bit):	6.937928587847823
Encrypted:	false
SSDEEP:	1536:PH/PuPigXWKQCLy2zmzNGBT3jjdhDV9Cmv2OavOiS8Q4WN8Y/gAyBzogt:23XWK7O2zm+rDVxeiN8YxK
MD5:	0BFF9E2A6E830163E8651B5DAFD9000C
SHA1:	A9766195D4831C368DCE50D94684422B01B5B1AA
SHA-256:	5EA98A6D50C5269153D27C95CC3350EBC6323B7E8C8FF40BE98C3365B6131AD0
SHA-512:	2B0863A3BC855EB733ACF6D6A98899201A327516FE15A5EA0BD1F4DDE31A9A73A1A58713561E70B2885E3F94A143CF8742D00606C714925BEF0527A6F4710A09
Malicious:	false
Reputation:	low
Preview:	.....`Exif..MM.*.....b.....j.(.....1.....r.2.....i.....O...'...O...'.Adobe Photoshop CS5.1 Windows.2012:03:28 10:01:36..... {.....&.(.....*.....H.....H.....Adobe_CM.....Adobe.d..... .....q..".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv..... .7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?../.....T,._.....?...Y?..x.p.._7..y.....k.. .~.....t|N.....].m.[o.[.y}.].5.....s.....Q.....S..O.^}-...w...~.....U...<9^Tb..f._.`.0|?$..rY#/p...T

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\649808E8.jpg	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=12, height=272, bps=0, PhotometricIntepretation=CMYK, orientation=upper-left, width=862], baseline, precision 8, 209x66, frames 3
Category:	dropped
Size (bytes):	51850
Entropy (8bit):	7.311126106804344
Encrypted:	false
SSDEEP:	768:iYy8DaCrYy8Dajc39NKk0YyMqHKS7HRBIkyc16mV:ioZoac39NKk0tNTRC8
MD5:	291D6B5D53C0FFF65D73620174A402D7
SHA1:	50C4B0DFFA0641BF03890C9D749AFBC6BD0F4E1D
SHA-256:	4600CB88A85D73DA87B52F076F46967D32FEAD53FD8E50C4C27812E2F5DD4E3A
SHA-512:	18D7C4318E7A8CF255E9E01FD8C3618D0F3F8A11105950A60F8812EA2B93C60B0D7A072D5F6C1DEFD0B7BE8952619B2DF93E861DA8CCD281431779940CC2DFI C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\649808E8.jpg	
Preview:	......Exif..MM.*.....^.....(.....1.....2.....i..... .....-....'..-....'.Adobe Photoshop CS5.1 Windows.2012:10:09 12:05:39.....0221.....B.....n.....v.(.....~.....H.....H.....XICC_PROFILE.....HLino....mntrRGB XYZ .....1..acspMSFT....IEC sRGB.....-HP .....cprt...P...3desc.....lwtpt.....bkpt.....rXYZ.....gXYZ...,....bXYZ...@....dmnd...T...pdmdd.....vued...L....view.....$lumi.....meas.....$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZ .....Q.....XYZ .....XYZ .....o...8.....XYZ .....b.....XYZ .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A82E41C3.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 240x240, segment length 16, baseline, precision 8, 1852x397, frames 3
Category:	dropped
Size (bytes):	81290
Entropy (8bit):	6.214869581114551
Encrypted:	false
SSDEEP:	1536:/MbKPHdX5Xmyiiiiiiiiiiiiiiiiiiiii4ioS1:/FHpiiiiiiiiiiiiiiiiii4ioS1
MD5:	662B972F0F7D2E8A756CF5D14B84A4E4
SHA1:	B503083BA125111783386527C6EEA35389263474
SHA-256:	F897C45EDADD81506F9E0C60DDF78AE900C09DEB73A186BAF7E053A57AFFF1FE
SHA-512:	B01EBD30AB78C8AC599262323910CF2C5A5E593845027CEE85DE1FE7A521D48EEED778030050C7558F2881F2B2E25537B71E7C0C02DDA05452A7C5D49CEB466
Malicious:	false
Reputation:	low
Preview:	......JFIF.....,Photoshop 3.0.8BIM.....Adobe.d..... .....<.....u.....!.."..1.A2#..QB.a$3.Rq..b.%C...&4r....5'.S6..DTsEF7Gc(UVW.....d.t..e.....)8f.u*9:HIJXYZghijvwxyz.....m.....!..1.."AQ.2a.q.B.#..R.b.3..$..Cr...4%.S.cD.&5.T6Ed'.s..Ft....UeuV7.....).....(GWf8v.....gw.....HXhx.....9IYiy.....*:JZjz.....?...'.....u...{.{.^....R....6..../...../.V7..U....$..o..$...FO..u`~.....u.~..{..^...s.g.....uy?....y.....yw.....b...=.....o..}/....Js.I..Y.....}.V.m.8....Q.....u...{.{.^.....u...{.{.^.....u...{.{.^.....u...{.{.^.....u...{.{.^.....u...{.{.^.....u...{.{.^.....u...{.{.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{291F1171-AE78-4EDC-B620-D7F249186DA8}.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\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B0ADB03E-3222-4B2B-A26F-2432C7ED640E}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	31744
Entropy (8bit):	4.35493791111299
Encrypted:	false
SSDEEP:	384:WvD+XZGOVyPtNl9Riw7DPk7spSDRfb/ZUQ:kDEZGOwtNlm6PiscRfKQ
MD5:	935E0613257DFA1CA8FA3A3D63BA70C0
SHA1:	D55BC803C08BC31ECDE5BDFBE0058ECBCFC6D40F
SHA-256:	AB96ACB0EDB10060A3BE3F737AA393B5196EF9FDD5238EB1B18BE840EDCC04E9
SHA-512:	FFE82191D900BAA4566ADCD2136407648A4E320EBAF8A703E6F1638F1123C83543952B3F0B45F8AE8F0AB255D57B4CD29A64DD16F4D42EF740273F5A16250A4E
Malicious:	false
Reputation:	low
Preview:	..... .!."#.$.%.&.'.(.).*.+.,.-.../.0.1.2.3.4.5.6.7.8.9.:.;.<.=.>...../.....H.e.a.l.t.h.S.h.a.r.e. .N.S.W. ...C.O.V.I.D.-.1.9. .S.a.f.e.t.y. .R.e.c.o.m.m.e.n.d.a.t.i.o.n.s. .f.o.r. .S.u.p.p.l.i.e.r.s.....D.a.t.e.:. .2.3...0.8...2.0.2.1.....P.u.r.p.o.s.e...T.h.e. .p.u.r.p.o.s.e. .o.f. .t.h.i.s. .d.o.c.u.m.e.n.t. .i.s. .t.o. .p.r.o.v.i.d.e. .g.u.i.d.a.n.c.e. .t.o. .H.e.a.l.t.h.S.h.a.r.e. .N.S.W. .(.H.S.N.S.W.).....:...<...>...@...B...D...H..... .....d....gd.4.....d....7$.8$.H$.gd.I.....$..d....a$.gd.I.....d....gdB=

C:\Users\user\AppData\Local\Temp\msoC6D8.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	GIF image data, version 89a, 15 x 15
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.949125862393289
Encrypted:	false
SSDEEP:	12:PlrojAxh4bxdtT/CS3wkxWHMGBJg8E8gKVYQezuYEecp:trPsTTaWKbBCgVqSF
MD5:	ED3C1C40B68BA4F40DB15529D5443DEC
SHA1:	831AF99BB64A04617E0A42EA898756F9E0E0BCCA
SHA-256:	039FE79B74E6D3D561E32D4AF570E6CA70DB6BB3718395BE2BF278B9E601279A
SHA-512:	C7B765B9AFBB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA878 41
Malicious:	false
Reputation:	high, very likely benign file
Preview:	GIF89a....w..!..MSOFFICE9.0.....sRGB.....!..MSOFFICE9.0.....msOPMSOFFICE9.0Dn&P3.!..MSOFFICE9.0.....cmPPJCmp0712.....!.....,.....'.;..b...RQ.xx.... .....,+.....yy..;..b.....qp.bb.....uv.ZZ.LL.....xw.jj.NN.A@....zz.mm.^_.....yw.....yx.xw.RR.,*.++..... .....8....>.....4567...=..../0123.....<9:.()*+,-.B.@...."#$%&'..... !..... .....C.?....A;<...HT(..;

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Appendix 2 210823_COVID Safe Checklist for Suppliers.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=Mon Aug 30 20:08:53 2021, mtime=Mon Aug 30 20:08:53 2021, atime=Sat Sep 25 11:33:10 2021, length=419908, window=hide
Category:	dropped
Size (bytes):	2458
Entropy (8bit):	4.578232004439867
Encrypted:	false
SSDEEP:	48:86PZH/XTKbM0kwHTmPwAGiWf26PZH/XTKbM0kwHTmPwAGiWB:88/XGbM0LzAGiWf28/XGbM0LzAGiWB
MD5:	723DAE0A09BAE8EC30E8EC14B7EF35CF
SHA1:	451EAABB4C7615555C72ECACA429457B180B9A4A
SHA-256:	FFE23C4AF2D19FBB0B3982D13095E372C7A1E5951CFCCD0BE2024915618245C5
SHA-512:	1F4751DAC0BCAD52EFBABF3F2A5CFEA2F3A0A81DE5284B83893CD851B4243A8016D9C70C8D92E32095A4818A9EBEC4E2711B1D3B4B472E6B3226D9CB0C13A 61
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....k.<....k.<...C.....Dh.....%....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.....S....user.8.....QK.X.S..*...&=....U.....A.l.b.u.s.....z.1.....S....Desktop.d.....QK.X.S..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-2.1 .7.6.9.....2.Dh..9S&d .APPEND~1.DOC.....S...S..*.....A.p.p.e.n.d.i.x. .2. .2.1.0.8.2.3._.C.O.V.I.D. .S.a.f.e. .C.h.e.c.k.l.i.s.t. .f.o.r. .S.u.p.p.l.i.e.r.s...d.o.c.x..... .....-...8...[.....?J.....C:\Users\..#.....\\141700\Users.user\Desktop\Appendix 2 210823_COVID Safe Checklist for Suppliers.docx.P.....\....\....\....\....\... ..\.D.e.s.k.t.o.p.\.A.p.p.e.n.d.i.x. .2. .2.1.0.8.2.3._.C.O.V.I.D. .S.a.f.e. .C.h.e.c.k.l.i.s.t. .f.o.r. .S.u.p.p.l.i.e.r.s...d.o.c.x.....:.,.LB.)...Ag.....1SPS.XF

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):	196
Entropy (8bit):	5.089552666256573
Encrypted:	false
SSDEEP:	6:HvZMVDEFcvaY6YvqaMVDEFcvaY6YyZMVDEFcvaY6Ys:HWVouAYUVouAY5VouAYs
MD5:	8123581FA19EA057B3D23F47C5245A07
SHA1:	2B118ABB4089DDA3FC9F982EBBBF769EE77E5959
SHA-256:	A4FC4C7B378B46E310D33188ABA49E5F018BF864D03B1FE98EC94E9FBA12D53B
SHA-512:	571DA10C22C9E7949C4FD866FBCB99B10DE287C185AF3CA213A42228FCD5D1BB51EA80D6D6EFAA40778254E71F82587E7B1D722335091725C41778E03BD2853
Malicious:	false
Reputation:	low
Preview:	[misc]..Appendix 2 210823_COVID Safe Checklist for Suppliers.LNK=0..Appendix 2 210823_COVID Safe Checklist for Suppliers.LNK=0..[misc]..Appendix 2 210 823_COVID Safe Checklist for Suppliers.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):	2.5038355507075254
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
SSDEEP:	3:vrJlaCkWtVyDFH5UKycWT5yAi/lln:vdsCkWtgZ2YAyll
MD5:	6525B5171CE36A6D7EDB3E4DFD5CB579
SHA1:	70AFC3864539BCF8F1C4CD336F6096534A6268FA
SHA-256:	617E1415F4483DAE29072F8E5A042E9EB3446F53F9AC2F26180AECD1D93151CF
SHA-512:	700AEAE11F026EDE01A59B5CC1166D041E1B100E91F84F984D072CDB154251AD15A11C629B8CD7314CB0B2FF8669C3C52EB592020FBA2502CB35BDE6D1EA832
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\Desktop\~$pendix 2 210823_COVID Safe Checklist for Suppliers.docx	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyDFH5UKycWT5yAi/lln:vdsCkWtgZ2YAyll
MD5:	6525B5171CE36A6D7EDB3E4DFD5CB579
SHA1:	70AFC3864539BCF8F1C4CD336F6096534A6268FA
SHA-256:	617E1415F4483DAE29072F8E5A042E9EB3446F53F9AC2F26180AECD1D93151CF
SHA-512:	700AEAE11F026EDE01A59B5CC1166D041E1B100E91F84F984D072CDB154251AD15A11C629B8CD7314CB0B2FF8669C3C52EB592020FBA2502CB35BDE6D1EA832
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.287130310103167
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:	Appendix 2 210823_COVID Safe Checklist for Suppliers.docx
File size:	419908
MD5:	351ca19e59770dccb7bd8500d7445c07
SHA1:	4c688de3fe209afd4c6a458c80292932f98a8e9f
SHA256:	5a426bd44b10b1fc4f2158f1f9fa07e0c047e2115b97542bfd4a5c33d30250fa
SHA512:	7bd1f964f5c6300dd06123a140a79543c1ea589c397c3b53e716c6b3a41194d4421573cb78fc3b7e47ab8114a77b2d63e0f1a95e64aec23ed57ab037998e985f
SSDEEP:	6144:9naLJiiiiiiiiiiiiiiiiiioNTRuGt+Vxe5YSWKW1n+:9nE/uW15CKW1n+
File Content Preview:	PK.....!.....[Content_Types].xml ...(.....

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 1180 Parent PID: 596

General

Start time:	05:33:10
Start date:	25/09/2021
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:	0x13fb90000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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