ID: 490191
Sample Name: Appendix 2 210823_COVID Safe Checklist for Suppliers.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 05:36:43
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

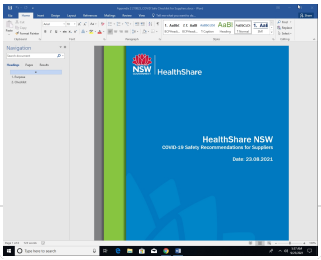
Windows Analysis Report Appendix 2 210823_COVID S…

Overview

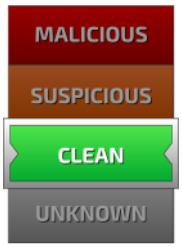
General Information

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

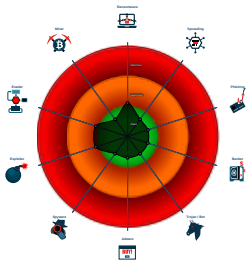


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 7032 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

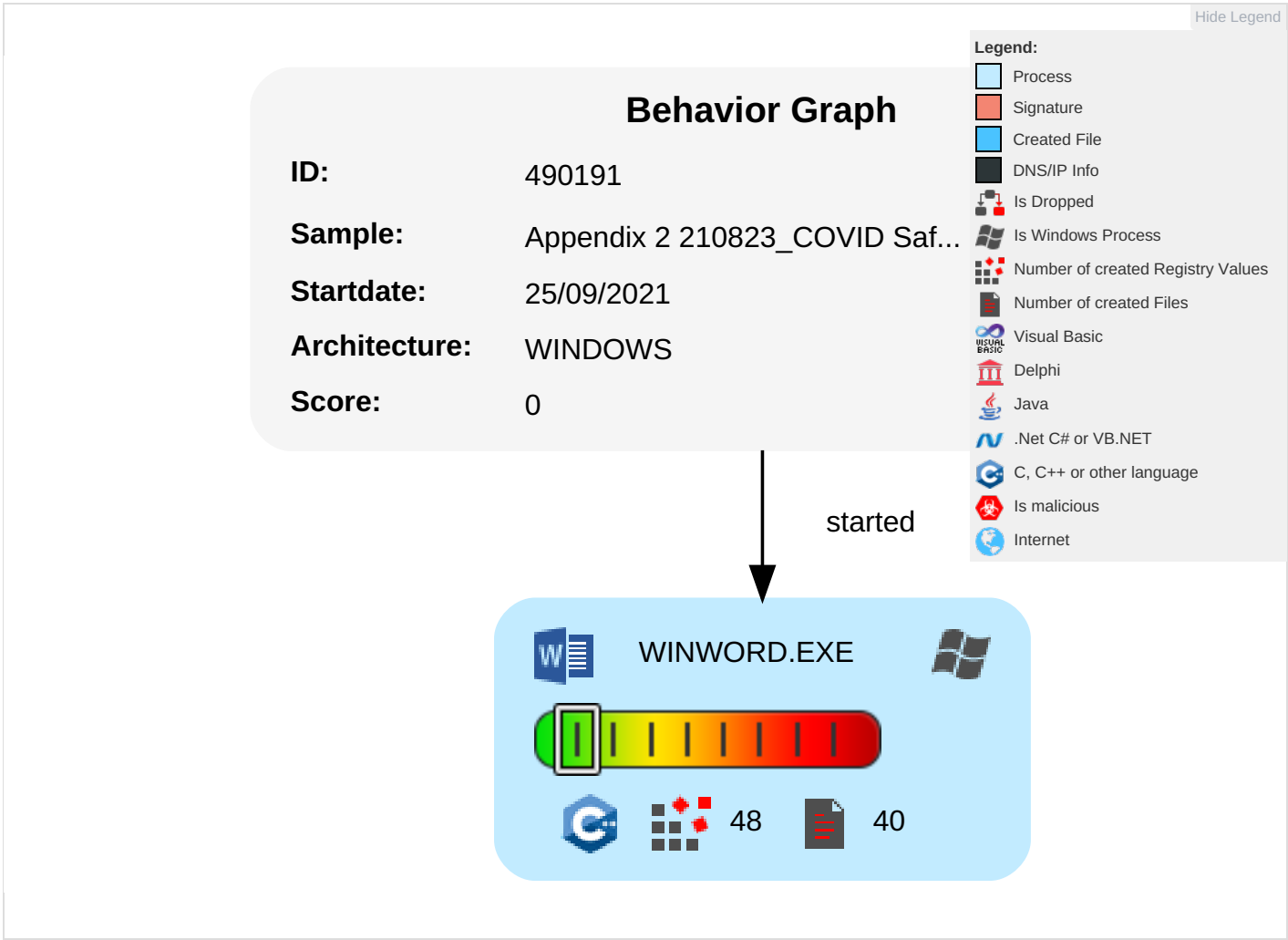
Click to jump to signature section

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	Extra Window Memory Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	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	Extra Window Memory Injection 1	LSASS Memory	System Information Discovery 2	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

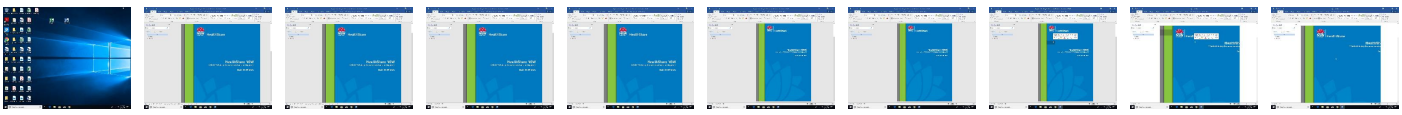
Behavior Graph

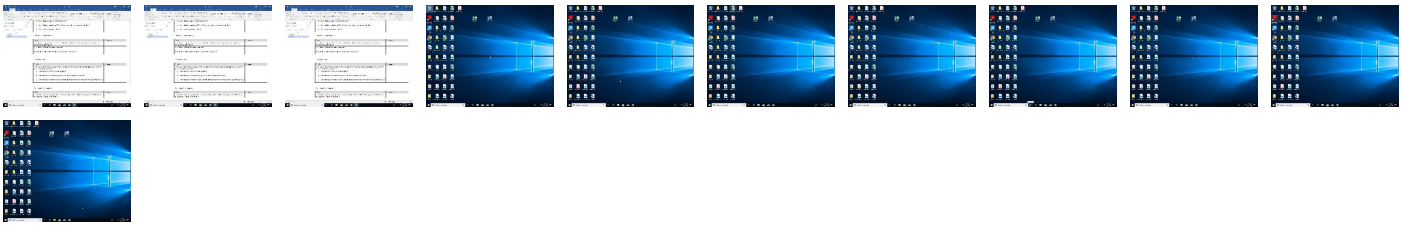


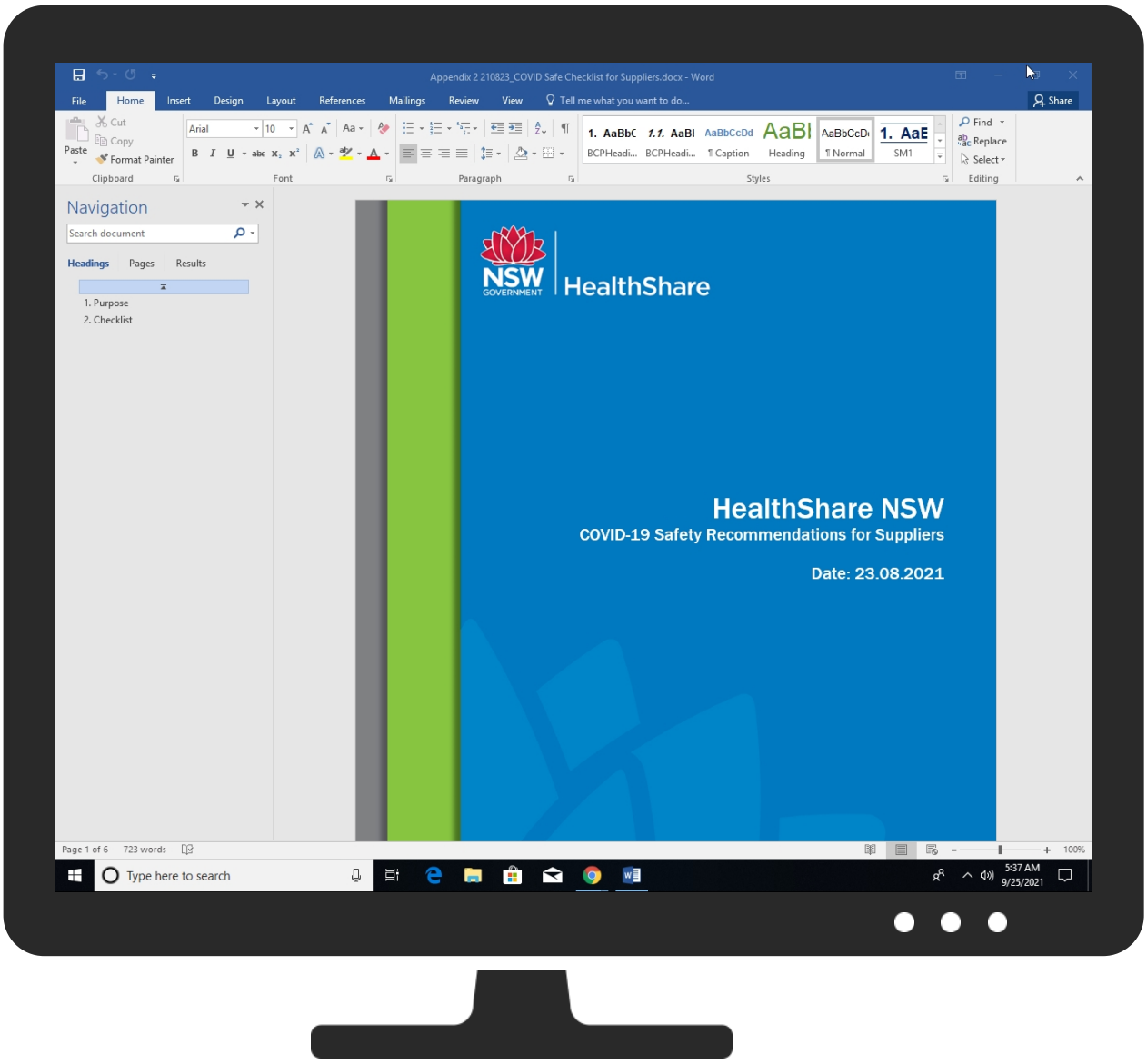
Screenshots

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

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-gcc.office.com;https://augloop.gov.online.office365.us;ht	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

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:	05:36:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 10s
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 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211

Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	23
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:	CLEAN
Classification:	clean0.winDOCX@1/11@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\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\A995F541-B2E4-422C-AACC-8E9820931BF3	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\A995F541-B2E4-422C-AACC-8E9820931BF3	
Size (bytes):	138701
Entropy (8bit):	5.360733957405008
Encrypted:	false
SSDEEP:	1536:RcQIKNZeBdA3gBwfnQ9DQW+z2Y34Zli7nXboOidX8E6LWME9:EWQ9DQW+z6Xh1
MD5:	68588703837A86C8C8D21C1308F5E12B
SHA1:	AE75E58F4ADCAC72300E006E94808D7302820C0D
SHA-256:	606E14F4112D7C99782C9251A7F9F33528687768E41BDF37D23ABBAE889FDDAA
SHA-512:	F0001789CFC720C2673227C601B62F14CD1A3B71E51D1BB3FD0189162D5EE10340D3BB9F560B5E2C2831605E3E57C8B7A05083451702449EF63C1683DA1B8F5F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-09-25T03:37:33">.. Build: 16.0.14522.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3A9E6B.jpeg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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\INetCache\Content.MSO\7C226EB1.jpg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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
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...p dmdd.....vued...L....view.....$lumi.....meas.....$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC 61966-2.1.....sRGB IEC61966-2.1.....XYZ .....Q.....XYZ .....XYZ .....o...8.....XYZ .....b.....XYZ .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D68BAD70.jpeg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D68BAD70.jpeg	
SSDEEP:	1536:/MbKPHdX5Xmyiiiiiiiiiiiiiiiiiiii4ioS1:/FHpiiiiiiiiiiiiiiiiiii4ioS1
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\INetCache\Content.Word\~WRS{0079D037-94AF-435C-838F-E3F9B1D0612F}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	31744
Entropy (8bit):	4.368228115334748
Encrypted:	false
SSDEEP:	384:71gJPR9pvvD1DPqmurgXZGOVyPtNl9Riw7DPk7spSDRfb/Z3YQ:0DvZGOwtNlm6PiscRfmQ
MD5:	B64F321FD16FA16C6FD6F023E3F7D2C9
SHA1:	18F98055D0ED9D9A7521DA8174CD91B1E527D0E0
SHA-256:	63341E0E0236527184F8E36E0FEFCA30548BE488AE3E76C707FB21901EC6D208
SHA-512:	19F161C8582DDB7546C0064DE0C2504EB4B2BAAEBA81E565914DB17177633AFA46ECE0171430BCD56CDBEA6AB3871F1AAB5D692B15BAD7F961F987A672D2AD 56
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\Microsoft\Windows\INetCache\Content.Word\~WRS{62E4CAA0-9452-4F14-977B-520F10F7470E}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\msoF18F.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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

C:\Users\user\AppData\Local\Temp\msoF18F.tmp	
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.docx.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Thu Sep 23 14:11:34 2021, mtime=Sat Sep 25 11:37:34 2021, atime=Sat Sep 25 11:37:31 2021, length=419908, window=hide
Category:	dropped
Size (bytes):	2540
Entropy (8bit):	4.691319481103152
Encrypted:	false
SSDEEP:	48:8COxwZvmmtwBbemB6pCOxwZvmmtwBbemB6:8COWOBbemKCOWOBbem
MD5:	F0C250F270FDE0F58AEC9A401087A4B7
SHA1:	8A656A3B4D73299560A5316EC1A8A5B4D0A8C7E8
SHA-256:	327834BAD371485DDCA4E215D5018E97D20739BA417CD9C1B0511A6FF3BEBCC2
SHA-512:	A5B231701A6F0996C351BD465C266DE4BB21B17318AE502DA71B53991B6280F4A9E30B0A15440DD216349AE8B1648974B9A06E6A7F4B25DCE6B869D8175FBABI
Malicious:	false
Preview:	L.....F.... ....2.K....s.2.....#u.....Dh.....5....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..9S.d.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....7Ssy..user.<.....Ny.9S.d.....S.....h.a.r.d.z.....~.1.....7Svy..Desktop.h.....Ny.9S.d.....Y.....>.....K...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.....7Sry9S.d....h.....j..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.....-.....~.....>.S.....C:\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.)...As...`.....X.....226546.....!a..%.H

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.112849347974913
Encrypted:	false
SSDEEP:	6:HvZMVDEFcvawjF/qaMVDEFcvawjFiZMVDEFcvawjFc:HWVoudFkVoudFpVoudFc
MD5:	43C7F9BB92912E9EFCAD7D8D424E8E4F
SHA1:	DF7F86B3FE971E3C1F7B22A0AAC42D6FF105592C
SHA-256:	BA4036B84FFF899357D3A5824C44D8417DDBBB0E25CA565D7B5FEB1C9EFFB953
SHA-512:	9E8F6C53420B3D1DE50E5AD0C781B447483C13803C4F95A2DF147FF10E2B1FA099F02655A702242CA6CEEE7FC77BF8182BD3291A8EDBCF929FE41CD8170AE4 7
Malicious:	false
Preview:	[misc]..Appendix 2 210823_COVID Safe Checklist for Suppliers.docx.LNK=0..Appendix 2 210823_COVID Safe Checklist for Suppliers.docx.LNK=0..[misc]..Appendix 2 210 823_COVID Safe Checklist for Suppliers.docx.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1834151436526175
Encrypted:	false
SSDEEP:	3:Rl/Zd/qXl1//7BXRlFlqK2sElctttoln:RtZ9q13BQAvOn
MD5:	8C5873161B7F499FAC145A2713FEE420
SHA1:	3A1619F8E751448C90217D65CA2BBD7CE66FDBF7
SHA-256:	6FE5AA268873E557CE642626135E64596BAC50D01383EB82970C1A358C35AAB5
SHA-512:	B579CDE65AE6F01FC31E0DAA05DE839484E1A34116FFC32BE5E4282D7975D09F2498EB92D0DEBF264DEAD2AB7DDE85B8A02532D42FDBF010619FDA86B3C24 71
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....I.....I.....$.....6C.....I.....

C:\Users\user\Desktop\~$pendix 2 210823_COVID Safe Checklist for Suppliers.docx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data

C:\Users\user\Desktop\~$pendix 2 210823_COVID Safe Checklist for Suppliers.docx	
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1834151436526175
Encrypted:	false
SSDEEP:	3:Rl/Zd/qXl1//7BXRlFlqK2sElctttoln:RtZ9q13BQAvOn
MD5:	8C5873161B7F499FAC145A2713FEE420
SHA1:	3A1619F8E751448C90217D65CA2BBD7CE66FDBF7
SHA-256:	6FE5AA268873E557CE642626135E64596BAC50D01383EB82970C1A358C35AAB5
SHA-512:	B579CDE65AE6F01FC31E0DAA05DE839484E1A34116FFC32BE5E4282D7975D09F2498EB92D0DEBF264DEAD2AB7DDE85B8A02532D42FDBF010619FDA86B3C24 71
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....l.....l.....$.....6C.....l.....

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:	5a426bd44b10b1fc4f2158f1f9fa07e0c047e2115b97542b fd4a5c33d30250fa
SHA512:	7bd1f964f5c6300dd06123a140a79543c1ea589c397c3b5 3e716c6b3a41194d4421573cb78fc3b7e47ab8114a77b2 d63e0f1a95e64aec23ed57ab037998e985f
SSDEEP:	6144:9naLJiiiiiiiiiiiiiiiiiioNTRuGt+Vxe5YSWKW1n+:9nE/ uW15CKW1n+
File Content Preview:	PK.....!.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 7032 Parent PID: 744

General

Start time:	05:37:31
Start date:	25/09/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x380000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
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 Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Disassembly