ID: 468641
Sample Name: Covid narrative 6.20 8.21 to bank.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 06:33:02
Date: 20/08/2021
Version: 33.0.0 White Diamond

Table of Contents

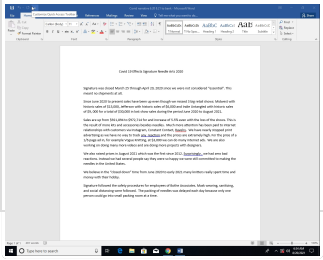
Windows Analysis Report Covid narrative 6.20 8.21 to b…

Overview

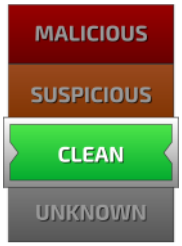
General Information

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

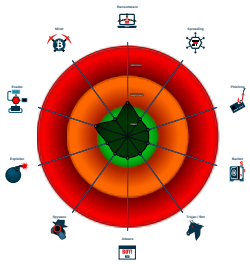


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 5860 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

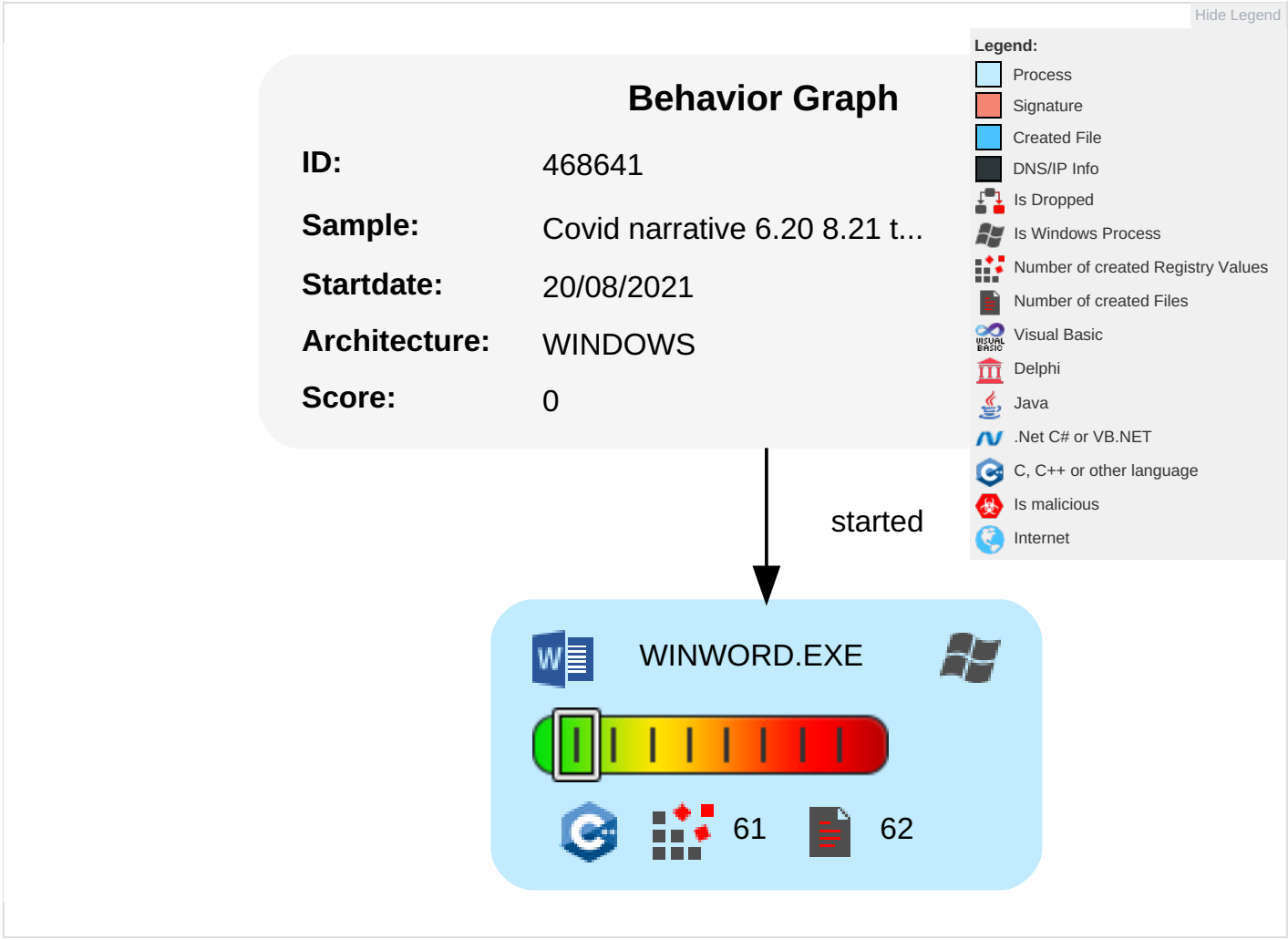
Click to jump to signature section

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	Path Interception	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	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

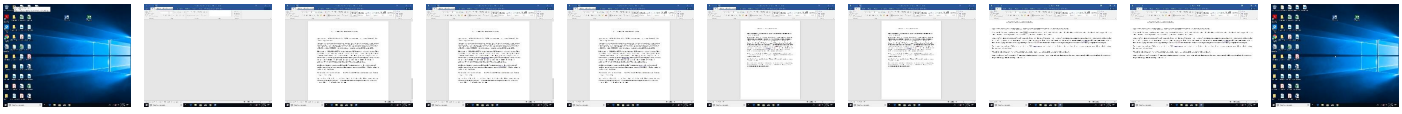
Behavior Graph

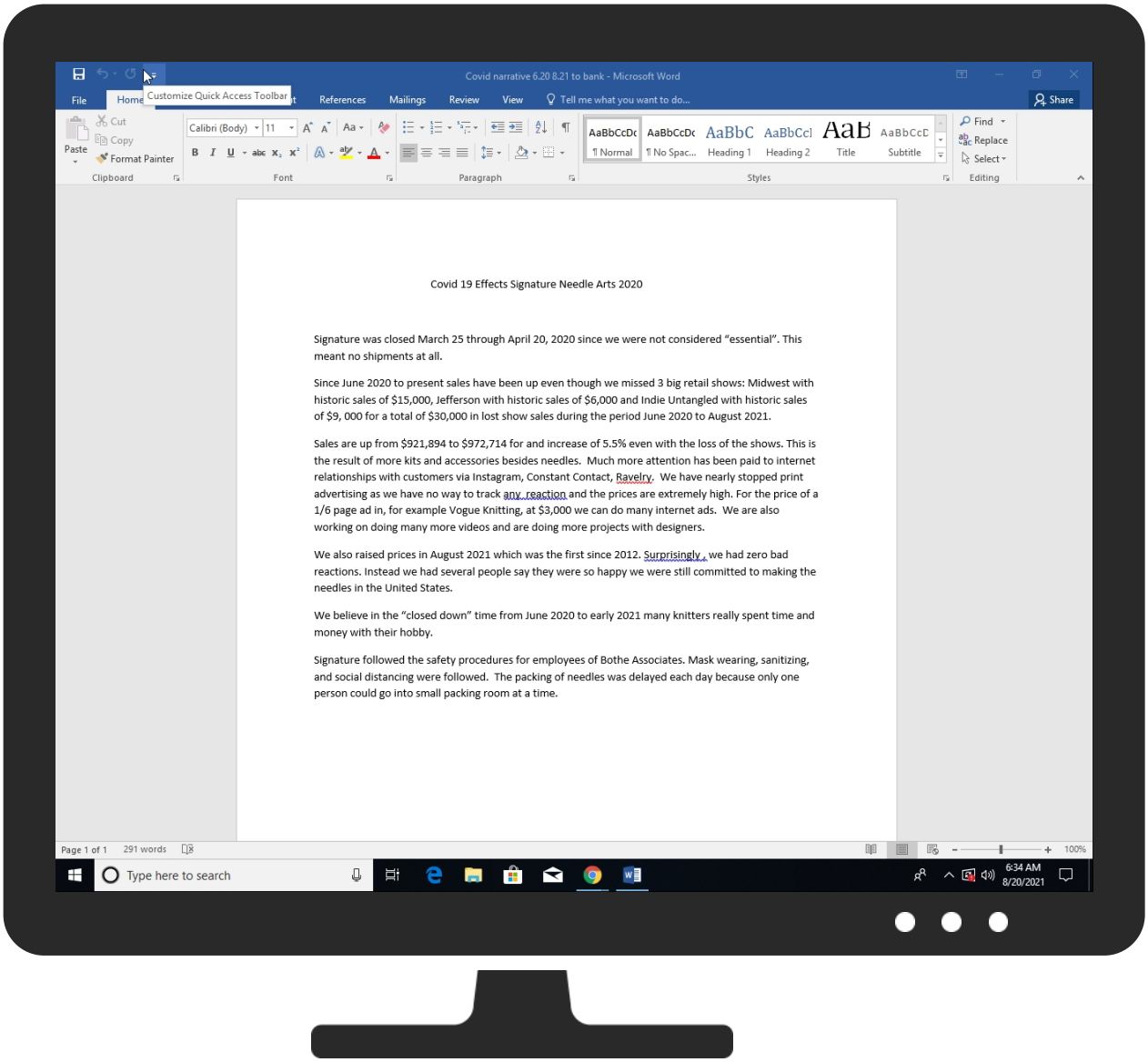


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Covid narrative 6.20 8.21 to bank.docx	0%	Virustotal		Browse

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://directory.services.	0%	URL Reputation	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:	468641
Start date:	20.08.2021
Start time:	06:33:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 42s
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 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:	19

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@1/23@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\88F4BA73-E444-42C8-A779-335BD740D924	
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
Size (bytes):	136730
Entropy (8bit):	5.361386637949192
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\88F4BA73-E444-42C8-A779-335BD740D924	
SSDEEP:	1536:lcQIKNveBQA3gBwbnQ9DQW+z2Y34ZliKWXboOidXqE6LWME9:PCQ9DQW+zaX31
MD5:	6731014807F36EBA1D7730909A3C87D1
SHA1:	3E63F304CB6689A4A9FEE277F52199834EC39500
SHA-256:	EC4A8AE9CE8D066B0291FE068CFE71EEC2B270A5710735568C173ADA3216E347
SHA-512:	43B6A3743BFDDA13481F29EA0E80E23760EF5830A8AD5AA6CAD8510282F7E1973C535FFCB5D1C7B71A0502CA40B1E98DA02454E9933BBB2965DBB962B5D3BF C
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="2021-08-20T04:34:06">.. Build: 16.0.14416.30525-->.. <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.Word\~WRS{8247A381-7F11-4245-93FB-912B508B9663}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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\Roaming\Microsoft\Bibliography\Style\APASixthEditionOfficeOnline.xsl	
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
Size (bytes):	333602
Entropy (8bit):	4.65455658727993
Encrypted:	false
SSDEEP:	6144:ybW83ob181+MKHZR5D7H3hgtfL/8mIDbEhPv9FHSVsioWUyGYmwxAw+GIfnUNv5J:Z
MD5:	58AAFDDC9C9FC6A422C6B29E8C4FCCA3
SHA1:	1A83A0297FE83D91950B71114F06CE42F4978316
SHA-256:	9095FE60C9F5A135DFC22B23082574FBF2F223BD3551E75456F57787ABC5797B
SHA-512:	1EBB116BAE9FE02CA942366C8E55D479743ABB549965F4F4302E27A21B28CDF8B75C8730508F045BA4954A5AA0B7EB593EE88226DE3C94BF4E821DBE4513118 A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">.. <xsl:output method="html" encoding="us-ascii"/>.... <xsl:template match="*" mode="outputHtml2">.. <xsl:apply-templates mode="outputHtml"/>.. </xsl:template>.... <xsl:template name="StringFormatDot">.. <xsl:param name="format" />.. <xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.. <xsl:when test="$format = ""></xsl:when>.. <xsl:when test="substring($format, 1, 2) = '%%'">.. <xsl:text>%</xsl:text>.. <xsl:call-template name="StringFormatDot">.. <xsl:with-param name="format" select="substring($format, 3)" />.. <xsl:with-param name=

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\CHICAGO.XSL	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	297017
Entropy (8bit):	5.000343845106573
Encrypted:	false
SSDEEP:	6144:GwprAtk0qvtfL/vF/bkWPz9yv7EOMBPitjASjTQQr7IwR0TnyDkJb78plJwf33iV:I
MD5:	0D0E65173F5AE6FE524DA09EEDDDCC84

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\CHICAGO.XSL	
SHA1:	C868617C86C1287B35875AE8D943457756B0B338
SHA-256:	787D1CBF076902B2568E8CFF1245E5FBEBA6AAD84240A54C4F9957084B93F90D
SHA-512:	E2FD5156BA707F6205B5CC52CC4FF8E1CDECB10B6C04E70EC4B3D3D0FA636AB9FDAE77F249D9D303D35CCCA8F8B399B60C602629B8803F708CFDAE8A11226 3D
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com :xslt" xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encodin g="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringForma tDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_E ndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</ xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" se lect="$p

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GB.XSL	
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
Size (bytes):	268670
Entropy (8bit):	5.054376958189988
Encrypted:	false
SSDEEP:	6144:JwprAJiR95vtfb8p4bgWPzDCvCmvQursq7vImej/yQzSS1apSiQhHDOruvoVeMUh:N4
MD5:	B17C7119B252FD46A675143F80499AA4
SHA1:	4445782BEC229727EE6F384EC29E0CBA82C25D22
SHA-256:	8535282A6E53FA4F307375BCEE99DD073A4E2E04FAF8841E51E1AA0EE351A670
SHA-512:	F9FB76A662DC6AB8DE22B87E817B4BAAC1AEEE08BA4F5090E6BC3060F42BC7CD15A71EB5B117554AEB395B22E5C2EEA7D0EFC36FF13BEC13B156879B87641 505
Malicious:	false
Reputation:	high, very likely benign file
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xs lt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us- ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormat Dot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_En dChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</x sl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" sel ect="$para

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostName.XSL	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	256358
Entropy (8bit):	5.104453150382283
Encrypted:	false
SSDEEP:	6144:gwprAB795vtfb8p4bgWPWEtTmtcRCDPThNPFQwB+26RxlsIBkAgRMBHcTCwsHe5a:BW
MD5:	4C7ECD0ED5ADCC30352E2C06931D290A
SHA1:	0E6A8E0EDDB5E67E26CF15692D1E8591F3D3D1DE
SHA-256:	40BACD32DB58799FA95B4707588ADEA1C9065CD804712B69B55DDD332C037D4E
SHA-512:	2C25363DCCDB718D427CE451963F1616344A59A57AF0A19F946B7C06536E773E0EA383AC48AAC35E109327B7B86432D608CB0490EBF9590A31AA87330D6F929E
Malicious:	false
Reputation:	high, very likely benign file
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft- com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="String FormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_p rop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>% </xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select=

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostTitle.XSL	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	251449
Entropy (8bit):	5.103599476769172
Encrypted:	false
SSDEEP:	6144:hwprA3R95vtfb8p4bgWPwW6/m26AnV9IBgIkqm6HITUZJcjUZS1XkaNPQTlvB2zr:XA
MD5:	234430F3D3032B9648671D3DF168D827

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostTitle.XSL	
SHA1:	4B7606E1F7E8172EE74DE90EE4CA75E3F44A0A2B
SHA-256:	DC7160C2FE5939E82BFEEE180C1DA8176C4914C034CAE8938ED6C9F7A9144F3E
SHA-512:	943119B65B2017F8FAAD5EC6B490CC8E263EC6128DD3D274A54EFB826FBE4353C72D335F5708974F1624E9BAE971C9D112905638B3F2123FC384DB201DE5B26
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ''"></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\HarvardAnglia2008OfficeOnline.xsl	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	284802
Entropy (8bit):	5.006325058456308
Encrypted:	false
SSDEEP:	6144:B9G5o7Fv0ZcxrStAtXWty8zRLYBQd8itHiYYPVJHMSo27hlwNR57johqBXlwNR2b:G
MD5:	08AD981C6D9BFD066BF29A77A62F0FEA
SHA1:	DBE60C2A2BC9A80EFBD6BE114BDF1416261C94E6
SHA-256:	BCFB2EF3D37F7DAFCB9FF4D92885C5F87B4BEC7A3045BC7208460DAE7DABAE31
SHA-512:	64A939705679AA9EBD66634059A63BE280DF197845F23334906EF419C891E1393700344EE8D200195B72509874AD6046495815B94C1BF998116C351BC483C6EB
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".....xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">.....<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="/">....<xsl:call-template name="Start"/>...</xsl:template>.....<xsl:template name="Start">....<xsl:choose>.....<xsl:when test="b:Version">.....<xsl:text>2010.2.02</xsl:text>.....</xsl:when>.....<xsl:when test="b:XslVersion">.....<xsl:text>2008</xsl:text>.....</xsl:when>.... <xsl:when test="b:StyleNameLocalized">.. <xsl:choose>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1033'">.. <xsl:text>Harvard - Anglia</xsl:text>.. </xsl:when>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1025'">.. <xsl:text>Harvard - Anglia</xsl:text>.. </xsl:when>.. <x

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\IEEE2006OfficeOnline.xsl	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	294525
Entropy (8bit):	4.978414555953716
Encrypted:	false
SSDEEP:	6144:ndkJ3yU0orh0SCLVXyMFsoiOjWIm4vW2uo4hfhf7v3uH4NYYP4BpBaZTTSSamEUD:Y
MD5:	96F3CCC20E23824F1904EDFDFE5CDA02
SHA1:	EF78E9B415A9FFD4094E525509D3AEB3E2A68EEE
SHA-256:	9970654851826C920261D52F8536B1305F7E582C7A2E892BAC344A95F909FE63
SHA-512:	1022D3E990B1A31361C9658C6C15DB9B41DA38E73319C93C62EE8E57E36333261F66897E1F0F6502EC28B780A9FC434E7F548178F3BC1D4463A44BCF508604E1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".....xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">.....<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="/">....<xsl:call-template name="Start"/>...</xsl:template>.....<xsl:template name="Start">....<xsl:choose>.....<xsl:when test="b:Version">.....<xsl:text>2010.2.02</xsl:text>.....</xsl:when>.....<xsl:when test="b:XslVersion">.....<xsl:text>2006</xsl:text>.....</xsl:when>.. <xsl:when test="b:StyleNameLocalized">.. <xsl:choose>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1033'">.. <xsl:text>IEEE</xsl:text>.. </xsl:when>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1025'">.. <xsl:text>IEEE</xsl:text>.. </xsl:when>.. <xsl:when test="b:StyleNameL

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\ISO690.XSL	
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
Size (bytes):	270642
Entropy (8bit):	5.074829646335759
Encrypted:	false
SSDEEP:	6144:JwprAi5R95vtfb8pDbgWPzDCvCmvQursq7vImej/yQ4SS1apSiQhHDOruvoVeMUX:WL
MD5:	831E5489F3047AFF2EFDFF758FA42FEC
SHA1:	F27C9E96D726464E802AD007FE749B8F27FF4525
SHA-256:	7914A8B4ADFDC9A6589ED181DE46D3D735676A38AA61B8FAFC0F862B9EC3A1CD
SHA-512:	B84800FAB9FDF2AEFACBFC14527BC8361459E5138309E11C1025CF61A855C481E77EF14623182F485F3122A40BA4F873E4300B8D8209D924E3E16646FA34BCB8
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\ISO690.XSL	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\ISO690Nmerical.XSL	
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
Size (bytes):	217578
Entropy (8bit):	5.069961862348856
Encrypted:	false
SSDEEP:	6144:AwprA3Z95vtf58pb1WP2DCvCmvQursq7vIme5QyQzSS1apSiQhHDlruvoVeMUwFj:4P
MD5:	7777C0173259D8F4A4F5E69C1461CA14
SHA1:	9C83B87C098AECF3CDFC1B5C4C78B696BF14A5E6
SHA-256:	A343D61BAB2F25D138BDCC57D33C4A83FD494A54EAF3DF0F539E3B51CFE011F1
SHA-512:	77BFD6F7D21AB9771DF1993FB9AB82BA6D5E900F0B846F0F11578313E8A99C99E095612510CBB07590367EADE9B31CF396B26ABA5E8380F3ABC0886FA02858B9
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>..... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$parame

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\MLASeventhEditionOfficeOnline.xsl	
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
Size (bytes):	255219
Entropy (8bit):	5.004117790808506
Encrypted:	false
SSDEEP:	6144:MwprA8niNgtfbzbOWPuv7kOMBLitjAUjTQLrYHwR0TnyDkHqV3iPr1zHX5T6SSXj:x
MD5:	C9460BEAF863E337428518DAF5C09C5C
SHA1:	76BE7E80D117A73A4FFC96682345EECE9A5C4D2A
SHA-256:	A69368BE9AC843B088D739F1573007E634D1068DB0AD9937A95FE7A0690C05E0
SHA-512:	9E4A7D3E019D182CD6CFF4947364DCF435EF3B40BA004A360260EDA0712839875CB797DBFCCCD9E50885EB10AEF8695052899E4BAC16423D0EECCF025CF6B0F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>...</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.....<xsl:variable name="prop_EndChars">.....<xsl:call-template name="templ_prop_EndChars"/>....</xsl:variable>.....<xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$parameters" />.....

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\SIST02.XSL	
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
Size (bytes):	251336
Entropy (8bit):	5.057713103491112
Encrypted:	false
SSDEEP:	6144:JwprA6sS95vtfb8p4bgWPzkhUh9I5/oBRSifJeg/yQzvapSiQhHZeruvoXMUw3im:u9
MD5:	DAE31FA14BC97723A87F126B5121BAE3
SHA1:	C6B5CFF442FCC8795A5AF0D69ACDA24497D9F4BE
SHA-256:	30F377F7AC24B022F52371ADA97CB057460265F4C8BDDBB521642B6E2462EE27
SHA-512:	AE6B8BB6FCF956E1973C9E40702CB1A86FD8AD6F87FA1C2D3A2113C2F8AEC2A495FE636D71786843496F37FF9DB3D2F0E034BC4014D9C379E4EA4CC9495BE97
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\SIST02.XSL	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\TURABIAN.XSL	
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
Size (bytes):	344662
Entropy (8bit):	5.023256859004611
Encrypted:	false
SSDEEP:	6144:UwprAwnsqvtfL/vF/bkWPRMMv7EOMBPitjASjTQQr7IwR0TnyDk1b78plJwf33iD:F
MD5:	F82561FF802442D12B8B77EC6EDC027E
SHA1:	EE7ED23C6EF8DA4968BA969FC094203D61065C0E
SHA-256:	5B7A52DFAA9C3E9E340E081178B54E827ED591AC27DC098C3985C94BDE5CABE9
SHA-512:	FA205BCD1D61226A940EA333B3B3EC43FB461E7683669A344403B543B9F699677A9E332827EC0160E81A8FBFD43CA61735A5C414EE7C17143DC9819A137044B5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$pa

C:\Users\user\AppData\Roaming\Microsoft\Office\MSO1033.acl	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	37730
Entropy (8bit):	3.124590972713577
Encrypted:	false
SSDEEP:	768:GatNbFeZKdogeyHMOeYhIVi+iOFOqbPXdEmanb:R/eLAhIVJb2
MD5:	B4BA58FCF11E23F371B16B979827F341
SHA1:	556536CB452FF3746783E6AF7558AF93B2542FDC
SHA-256:	8469B5680A0B448D7C5033E9A97B8FFA718E9142C287DAE12E68FA496D8B34B6
SHA-512:	3394E23CCB822D65BCE0F4F1BE0ED23EE5F3C26C28CA95C80635B3641BA4BA48536251186C02B14838546504ECFBDE3DA1552D8A207487DA2D2894C10AAD643B
Malicious:	false
Preview:	.....w..b.....R.....(.c.).....(.e.)..... ....(.r.).....(.t.m.)....."!.....& ....a.b.b.o.u.t.....a.b.o.u.t.....a.b.o.t.u.....a.b.o.u.t.....a.b.o.u.t.a.....a.b.o.u.t. .a.....a.b.o.u.t.i.t.....a.b.o.u.t. .i.t.....a.b.o.u.t.t.h.e.....a.b.o.u.t. .t.h.e.....a.b.s.c.e.n.c.e.....a.b.s.e.n.c.e.....a.c.c.e.s.o.r.i.e.s.....a.c.c.e.s.s.o.r.i.e.s.....a.c.c.i.d.a.n.t.....a.c.c.i.d.e.n.t.....a.c.c.o.m.o.d.a.t.e.....a.c.c.o.m.m.o.d.a.t.e.....a.c.c.o.r.d.i.n.g.t.o.....a.c.c.o.r.d.i.n.g. .t.o.....a.c.c.r.o.s.s.....a.c.r.o.s.s.....a.c.h.e.i.v.e.....a.c.h.i.e.v.e.....a.c.h.e.i.v.e.d.....a.c.h.i.e.v.e.d.....a.c.h.e.i.v.i.n.g.....a.c.h.i.e.v.i.n.g.....a.c.n.....c.a.n.....a.c.o.m.m.o.d.a.t.e.....a.c.c.o.m.m.o.d.a.t.e.....a.c.o.m.o.d.a.t.e.....a.c.c.o.m.m.o.d.a.t.e.....a.c.t.u.a.l.y.l.....a.c.t.u.a.l.l.y.....a.d.d.i.t.i.n.a.l.....a.d.d.i.t.i.o.n.a.l.....a.d.d.t.i.o.n.a.l.....a.d.d.i.t.i.o.n.a.l.....a.d.e.q.u.i.t.....a.d.e.q.u.a.t.e.....a.d.e.q.u.i.t.e.....a.d.e.q.u.a.t.e.....a.d.n.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Covid narrative 6.20 8.21 to bank.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=Wed Sep 30 14:27:00 2020, mtime=Fri Aug 20 12:34:07 2021, atime=Fri Aug 20 12:34:03 2021, length=13120, window=hide
Category:	dropped
Size (bytes):	2376
Entropy (8bit):	4.6801274857038795
Encrypted:	false
SSDEEP:	24:8qf3yA/8fFHqDLF77aB6myqf3yA/8fFHqDLF77aB6m:8qp/csFiB6pqp/csFiB6
MD5:	43022D1651A4B70C58527A017B2F3415
SHA1:	491BA69CCBB6249793BA7603E266839548E07625
SHA-256:	B70609990708BDD4FB9A0756305B9822293B729725A178A12A33EC71A48A07B0
SHA-512:	F24158224D620C28673CCBF7B17FE6DFB9B8B8474250BA7C91B6EE6CA45110A75A6C28201A2F40B319BDCFF1A07286F049BA9DAC7BF49AA2C53F837E6DD4163
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Covid narrative 6.20 8.21 to bank.LNK	
Preview:	L.....F.... ....r.$>...QP.....).....@3.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...S8l.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....Z.1.....>Qb{..user..B.....N...S8l.....S.....Z...e.n.g.i.n.e.e.r.....~.1.....>Qe{..Desktop.h.....N...S8l.....Y.....>.....s.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l..,.-.2.1.7.6.9.....2.@3...SBl .COVIDN~1.DOC..~.....>Qa{.SBl.....R.....&.C.o.v.i.d. .n.a.r.r.a.t.i.v.e. .6...2.0. .8...2.1. .t.o. .b.a.n.k...d.o.c.x.....o.....-.....n.. .....>.S.....C:\Users\user\Desktop\Covid narrative 6.20 8.21 to bank.docx..=.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.v.i.d. .n.a.r.r.a.t.i.v.e. .6...2.0. .8...2.1. .t.o. .b.a.n.k...d.o.c.x.....:.,.LB.)...A}..`.....X.....992547.....!a..%.H.VZAj.....1.....-$..!a..%.H.VZAj.....1.....-$.....1SPS.XF.L8C..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Templates.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, Directory, ctime=Fri Aug 20 12:34:05 2021, mtime=Fri Aug 20 12:35:09 2021, at ime=Fri Aug 20 12:35:09 2021, length=0, window=hide
Category:	dropped
Size (bytes):	1177
Entropy (8bit):	4.67707013521467
Encrypted:	false
SSDEEP:	24:8VSA0Lc306omTK99A+8buTYa+/77aB6m:8VAIE69Wg+QuTF+/iB6
MD5:	796994024505A2BABB19B813302EA8BB
SHA1:	3CAE915AA0F89F11227BEFB89FD4031E29D87692
SHA-256:	E878F23FC35ED66A4507FECCC7C03692CB3F71EBD85ABDB98374DC0BF1DA8B32
SHA-512:	F468D775191BCC7FDE3A281FA622CA6EBFA94AFC5DB8612C4FE9D3961A456D07B5CBD0B7F03309078DCA9988CA60F8074DEEBD13DFAE5DC838852B14DB03DCCA
Malicious:	false
Preview:	L.....F.....'$.....bh.1.....1.....e....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...S8l.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....Z.1.....>Qb{..user..B.....N...S8l.....S.....Z...e.n.g.i.n.e.e.r.....V.1.....N....AppData.@.....N...S8l.....Y.....t..A.p.p.D.a.t.a.....V.1.....N..Roaming.@.....N...S8l.....Y.....D...R.o.a.m.i.n.g.....\.1.....SEl..MICROS~1..D.....N...Sel.....Y.....(.M.i.c.r.o.s.o.f.t.....\.1.....Sel..TEMPLA~1..D.....SCl.Sel....U.....K._.T.e.m.p.l.a.t.e.s.....d.....-.....c.....>.S.....C:\Users\user\AppData\Roaming\Microsoft\Templates.....\.....\.T.e.m.p.l.a.t.e.s.....>.e.L.:..er.=....`.....X.....992547.....!a..%.H.VZAj.....1.....-$..!a..%.H.VZAj.....1.....-$.....1SPS.XF.L8C....&.m.q....

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):	118
Entropy (8bit):	4.8662981454113705
Encrypted:	false
SSDEEP:	3:HtlwH4MTWpn8eHELkBVom41MwH4MTWpn8eHELkBVopnbJlv:HtlwYLhHiOV9wYLhHiOViv
MD5:	E34F83E3EAE91C05AB9A395CB6BA9642
SHA1:	186739A7148400917131A9CFF8ABAAC26E9139CA
SHA-256:	F311DB61261DCEEB5210240E803C1B64A28AEBBD25A68E2A8AB6F1E93F14DC5F
SHA-512:	D668D393A56E888AE8928318597F9B12FF92A3B2B9A0F6BBAC79DBF04F9C75E94CDF093C2B37C53F15EC98528F057A3F6853D0C0E850D74A8AFE8D02D94D747
Malicious:	false
Preview:	[misc]..Covid narrative 6.20 8.21 to bank.LNK=0..[folders]..Covid narrative 6.20 8.21 to bank.LNK=0..Templates.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\Normal.dotm (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	17940
Entropy (8bit):	7.405774188789956
Encrypted:	false
SSDEEP:	384:KaN8PC78FSiCo/6akwLWdxdlpeB/od8eTBtORsKP+bnm:oQ8Yi2akw6LlpeC1sRhPKm
MD5:	B14C80D825E9B3303FE2D03FB2E73CC1
SHA1:	14806B8633354277556BC2BE7B58AC0DC59B2F71
SHA-256:	F44B4A55450DC4084D5B8E3E69C33C49BAEAC9D87811E5B5DA260CFEB36E20EA
SHA-512:	CFA6CAAC2AC955529713CEF2BA48B4BCEF0E8CD6EB89FDE1608CF6F22C2BD0C8EA72ECFFFF8099069112DAD9D466424901BCDFB030AB192487E96AA6003CAB04
Malicious:	false
Preview:	..N.0.E.H.C.-J\X .....J..0....K.....H...R*.D.g..3.H....M!`.l.....J.j;*...>.b.Fa...B....wz...<`F..K6.._s.r.F`.<X.T....7....U.._t:.\:...<&....A%&:f.9..H.hd..*1y.Lx.k)".....e..k.g.....)....&.....A...3..WNN.U..e...<....'4(.....x.....nh.t.....p7..j..s...l@.w6.X..C.Tp...r+..^..F.N...".az...h.[!F.!...g...i"...C..n9.~l...3.....H..V..9.2.,)s..GZD..mo6M..a.!...q$.....O..r-.....PK.....!.Q3.p.....[Content_Types].xml ...(.....j.0.@....Q....N/c.....[

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Size (bytes):	162
Entropy (8bit):	3.1799377215974927
Encrypted:	false
SSDEEP:	3:Rl/ZdHDz6TEct1lrzlTBlnleKBpfWYRel:RtZ8TEctvrzhZBWYYl
MD5:	519AEC5E6B994A8FB444A2500E2B3082
SHA1:	934169671A96985D6BFFBEB1C80457768A88EEE9
SHA-256:	CB2439A9808E3465B9AB338F5D8A0E2C370CAA37001EA44B1C3A7000CB023005
SHA-512:	A1E9D0467F2A148E3C6D12FAFEFC74FB651B36F06C1500C4DDA32C61278172762F58EE4918B0BBD4272E6EC448AAE6504B446DD21377881347C55203CF74A4F
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....H/.B.F....U6.....h.....6.hr.lD/.B.G..o.l.e.3.2...d.l.l.....@/.B.H....S.i.g.n.a.

C:\Users\user\AppData\Roaming\Microsoft\Templates\~WRD0000.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	17940
Entropy (8bit):	7.405774188789956
Encrypted:	false
SSDEEP:	384:KaN8PC78FSiCo/6akwLWdxdlpeB/od8eTBtORsKP+bnm:oQ8Yi2akw6LlpeC1sRhPKm
MD5:	B14C80D825E9B3303FE2D03FB2E73CC1
SHA1:	14806B8633354277556BC2BE7B58AC0DC59B2F71
SHA-256:	F44B4A55450DC4084D5B8E3E69C33C49BAEAC9D87811E5B5DA260CFEB36E20EA
SHA-512:	CFA6CAAC2AC955529713CEF2BA48B4BCEF0E8CD6EB89FDE1608CF6F22C2BD0C8EA72ECFFFF8099069112DAD9D466424901BCDFB030AB192487E96AA6003CA B04
Malicious:	false
Preview:	..N.0.E.H.C.-J\X .....J..0....K.....H...R*.D.g..3.H....M!`.l.....J.j;*...>.b.Fa...B....wz...<`F..K6.._s.r.F`.<X.T....7....U.._t:.\:...<&....A%&:f.9..H.hd..*1y.Lx.k)".....e..k.g.....)....&.....A ...3..WNN.U..e...<....'4(.....x.....nh.t.....p7..j..s...l@.w6.X..C.Tp...r+..^..F.N...".az...h.[!F.!...g...i"...C..n9.~l...3.....H..V..9.2.,)s..GZD..mo6M..a.!...q$.....O..r-.....PK.....!.Q3. p.....[Content_Types].xml ...(..... ....j.0.@....Q....N/c.....[

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~$vid narrative 6.20 8.21 to bank.docx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.1799377215974927
Encrypted:	false
SSDEEP:	3:Rl/ZdHDz6TEct1lrzlTBlnleKBpfWYRel:RtZ8TEctvrzhZBWYYl
MD5:	519AEC5E6B994A8FB444A2500E2B3082
SHA1:	934169671A96985D6BFFBEB1C80457768A88EEE9
SHA-256:	CB2439A9808E3465B9AB338F5D8A0E2C370CAA37001EA44B1C3A7000CB023005
SHA-512:	A1E9D0467F2A148E3C6D12FAFEFC74FB651B36F06C1500C4DDA32C61278172762F58EE4918B0BBD4272E6EC448AAE6504B446DD21377881347C55203CF74A4F
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....H/.B.F....U6.....h.....6.hr.lD/.B.G..o.l.e.3.2...d.l.l.....@/.B.H....S.i.g.n.a.

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:	b77efefb8a22a24a9adb7ac682209f9a0b586a548008c6eb75978f4869fa439e
SHA512:	4826db406e2af4bc380b5a0024285be04d14177b5c8b905849c30eba7ad7eac80eba29c55b38433bccec835872986ae3c1c101fb75464873d0bcfd239986a79d
SSDEEP:	192:CtEvGREJ+nKFg5oCIo/lQ0reOmoWMuKFT+spo0IfFxDNxpZgo7M/wC:aEvlJTi5oDMlH7RNosBIfZGo4wC
File Content Preview:	PK.....!....IZ... .....[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: 5860 Parent PID: 792

General

Start time:	06:34:04
Start date:	20/08/2021

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:	0x3a0000
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 Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Disassembly