ID: 491720
Sample Name: Business Account 395022 Non Taxable.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:46:38
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

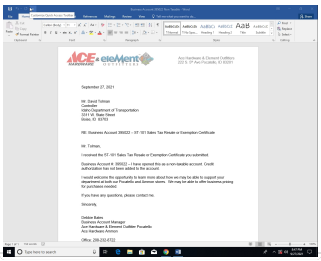
Windows Analysis Report Business Account 395022 No…

Overview

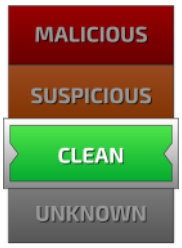
General Information

Sample Name:	Business Account 395022 Non Taxable.docx
Analysis ID:	491720
MD5:	ba70eb4f3ca9df3..
SHA1:	673ef069a308bf2..
SHA256:	e9947191baba0e..
Infos:	

Most interesting Screenshot:



Detection

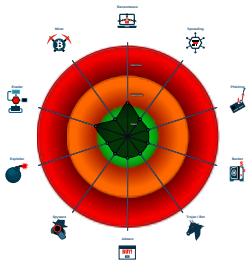


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 6128 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

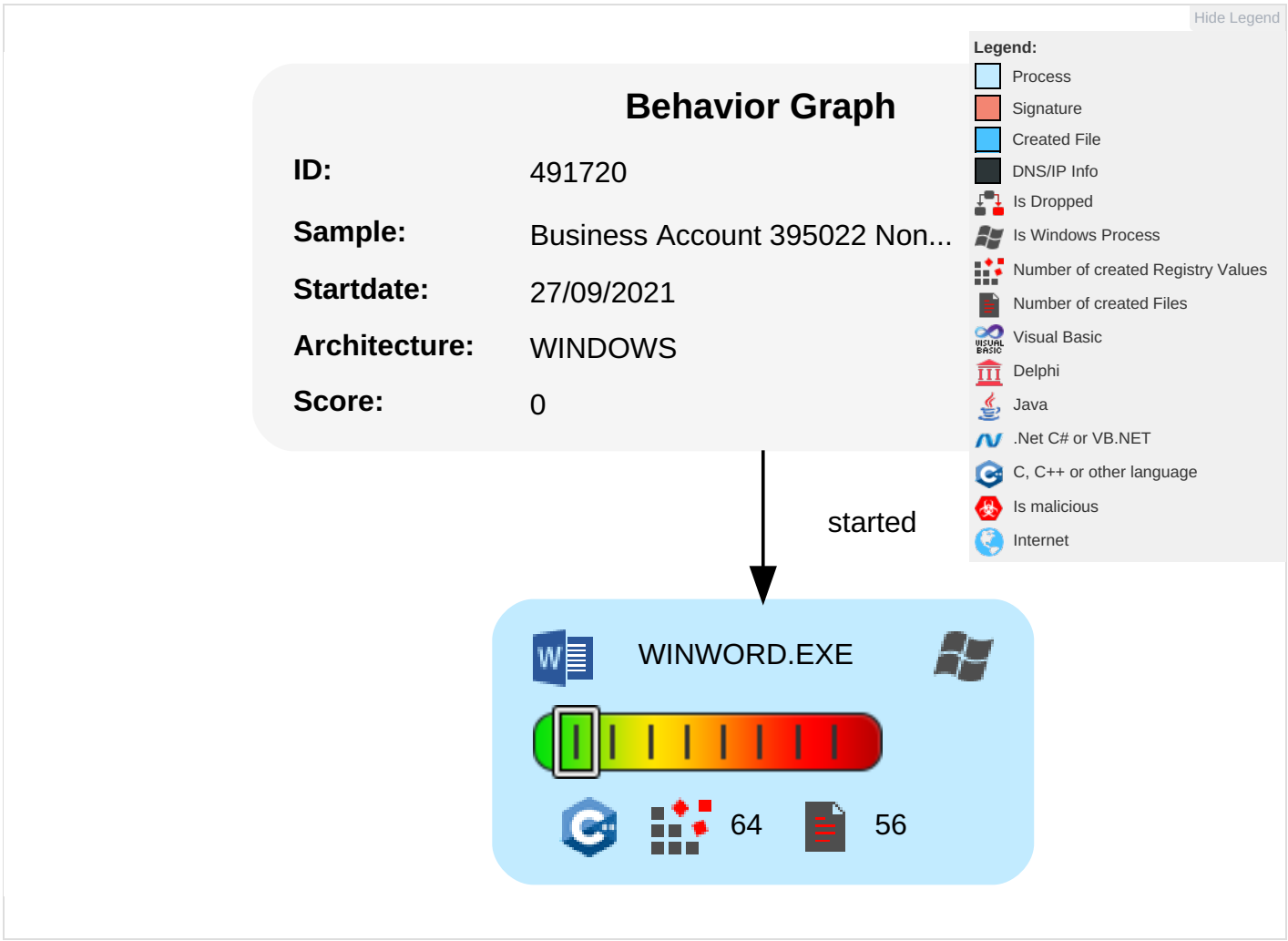
Click to jump to signature section

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 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

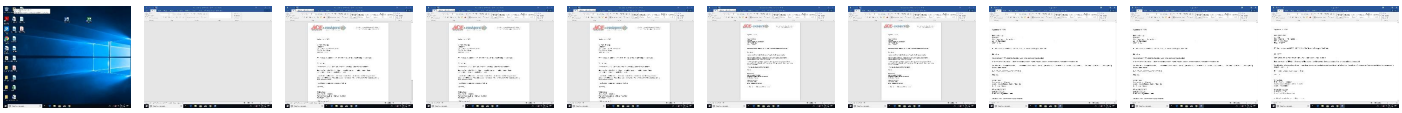
Behavior Graph

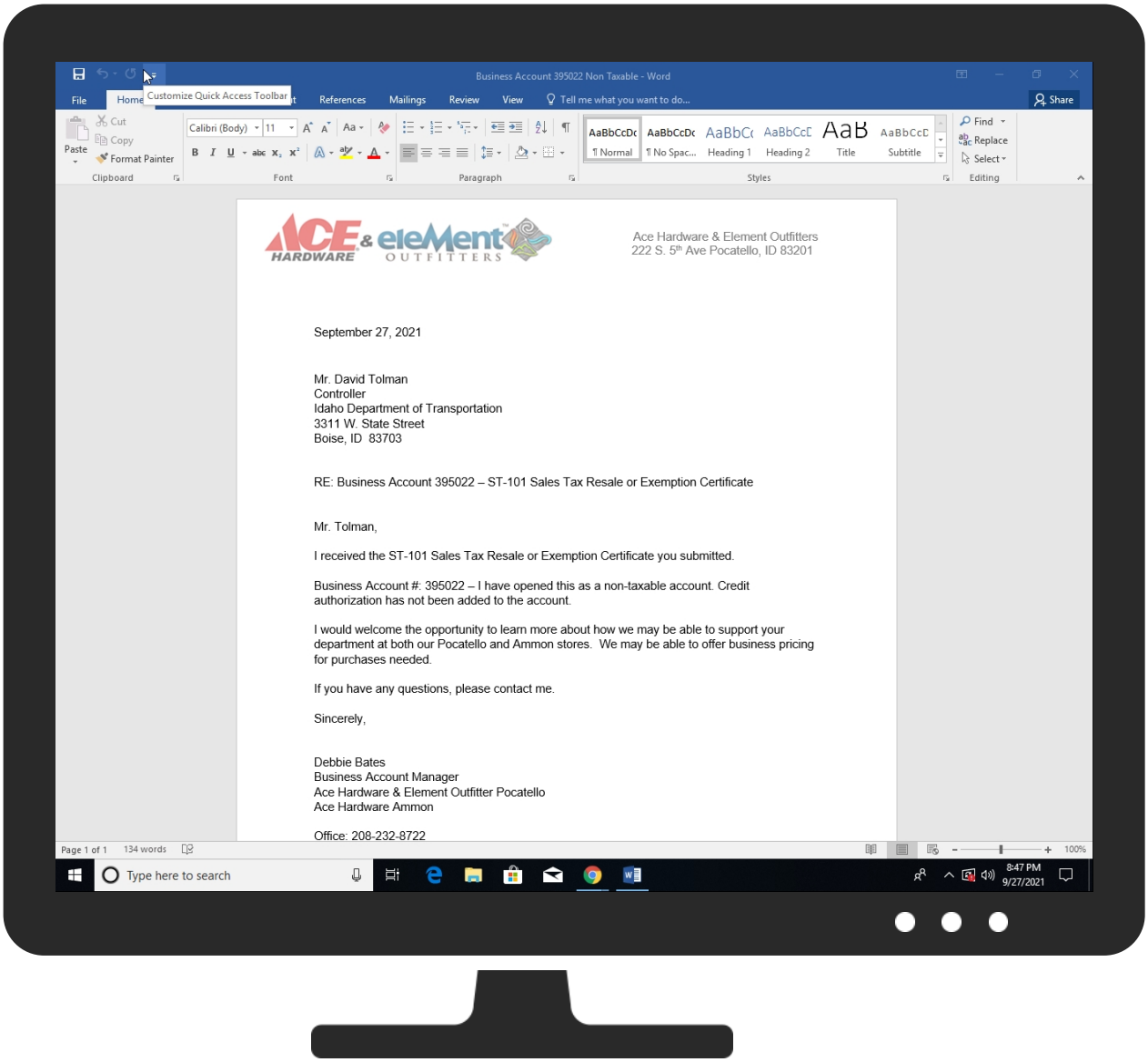


Screenshots

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:	491720
Start date:	27.09.2021
Start time:	20:46:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Business Account 395022 Non Taxable.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@1/24@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\ADC84891-67F2-48E7-933B-006235A591A3	
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):	138701
Entropy (8bit):	5.3607451390910645
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\ADC84891-67F2-48E7-933B-006235A591A3	
SSDEEP:	1536:KcQIKNZeBdA3gBwfnQ9DQW+z2Y34Zli7nXboOidX8E6LWME9:5WQ9DQW+z6Xh1
MD5:	4A4C389A698D2936823A170F83C70B38
SHA1:	6C67D73EB42BE80CCA82DFFDB6D85CEC1FCD579F
SHA-256:	E3784B25D8AA5D71765A6C09C7351B9D1160EE66FB7BC12CF222EF0D6397FD2E
SHA-512:	A1876A096A16166D11E52CF33B906F3DA808D7C0E9A3C475B8AAC1EB5942A2E1358D5F018986599B6C121CE3B6E541166A9FD6631FD70C49A5C9CFD22EE7260
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="2021-09-27T18:47:40">.. 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\DF284D01.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 574 x 115, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	49981
Entropy (8bit):	7.986631326847509
Encrypted:	false
SSDEEP:	1536:L8b6UrX/PJg79A8WJ53cbQj7ZxzgWGJMCAMC:Lq/Pw1WJ53cbqfs1JMCAj
MD5:	DAC4CD9C7DD1F15BD56F2E534A807E1D
SHA1:	4E95C3AD604068E278F6EF86A92CA140C94F00BD
SHA-256:	B6CBC23F0A9A10E947BF51C6F9E0DCE9BCDE60A3C9928FDB839224B0C83EAECA
SHA-512:	2F2049379CD3E43B2AE62F61306448F6ADD5D030125D6ACADD8980D021226C4C7847371D518496091A9268B6D6CE6ED58A1E8EA161301D287E023E7CEF5553A
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...>...s.....k.7....sRGB.....gAMA.....a.....pHYs.....&.?....IDATx^.].`T.....B.....ww.@...qw.b.....]..{\!..I...}3{w4.._.....{o~.;;+.... .)HA.R.....GA.R.... ..gH.|.. .)HA.R.....GA.R.... ..gH.|.. .)HA.R.....GA.R.... ..gH.|.. .)HA.R.....GA.R.... ..gH.|.. .)HA.R.....GA.R.... ..gH.|.. .)HA.R.....GA.R.... ..gH.|>.^.....=<.../..dw.. .)HA.R.?.....ea!....)S.}.0^..R.... .)HA.lR..O....q...qM....x..'.FA.R.... ..SI.|>.....DW....*x0v,..<.}. .)HA.R.....>.I.....I...+nJ$.RVF..#...eO(HA.R.....*)..GP.gx.d1.[4ET...+U.3>).... .1.S.R.... .).J.....O7oFb.....T...ok....9..^../^.V.... .)HA.DR... .4...#y.@D.+..*.....|.AT.r....<....g...R.... ...TTT...l./.....^.D.....].,bk}K..b....U. .Je.9;..v.,..#../.?...|.x..EO.....(HKG Aj..R..sv....=~.....E,...|.. .)HA..b.s..i.^...7n.k...I...$..y....4.;.[]..eU...D...z....._.2R4.{.,..L.V^df. 1Q..o..R..4c:....Q~....Wgd.....7.....<.?...Cyv...._FaF... .)HA...SNN.....4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{D33B3226-76BF-43EB-AFC1-9EADBC48AB7A}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	3.109799471692381
Encrypted:	false
SSDEEP:	48:6hUaL53+tEkXq1gIiwJCcENsgoR8djwZgs90Zy0Tqsj1jy:6hCTXq1gxqusncjwZQZjxy
MD5:	C90BE5FBE74CF4D109CCAAD98152B0CD
SHA1:	DAE640C23BE0F086578D26D40DAAF567A617009E
SHA-256:	2DF4B84E8819EB390C706585C96F4FAD86678EA2BDA53F8C410471CC8139F327
SHA-512:	DAB18F0691AC170309FE9796A09A3386DDF8B91C6E71D6B586CE91A0B2E2AC006300DB0401BDCBBCCD671E5D285F6712DAAABAFE35E06CC3503BA7453D98D D2B
Malicious:	false
Reputation:	low
Preview:	......S.e.p.t.e.m.b.e.r. .2.7.,. .2.0.2.1.....M.r... .D.a.v.i.d. .T.o.l.m.a.n...C.o.n.t.r.o.l.l.e.r...I.d.a.h.o. .D.e.p.a.r.t.m.e.n.t. .o.f. .T.r.a.n.s.p.o.r.t.a.t.i.o.n...3.3.1.1. .W... .S.t.a.t.e. . S.t.r.e.e.t...B.o.i.s.e.,. .I.D. . .8.3.7.0.3.....R.E.:. .B.u.s.i.n.e.s.s. .A.c.c.o.u.n.t. .3.9.5.0.2.2. .. .S.T.-.1.0.1. .S.a.l.e.s. .T.a.x. .R.e.s.a.l.e. .o.r. .E.x.e.m.p.t.i.o.n. .C.e.r.t.i.f.i. c.a.t.e.....M.r... .T.o.l.m.a.n.,.....P...f.....:...<..... ....

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

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\APASixthEditionOfficeOnline.xsl	
SHA-512:	1EBB116BAE9FE02CA942366C8E55D479743ABB549965F4F4302E27A21B28CDF8B75C8730508F045BA4954A5AA0B7EB593EE88226DE3C94BF4E821DBE4513118A
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
SHA1:	C868617C86C1287B35875AE8D943457756B0B338
SHA-256:	787D1CBF076902B2568E8CFF1245E5FBEBA6AAD84240A54C4F9957084B93F90D
SHA-512:	E2FD5156BA707F6205B5CC52CC4FF8E1CDECB10B6C04E70EC4B3D3D0FA636AB9FDAE77F249D9D303D35CCCA8F8B399B60C602629B8803F708CFDAE8A112263D
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($format, 3)" />.....<xsl:with-param name="parameters" select="$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:	F9FB76A662DC6AB8DE22B87E817B4BAAC1AEEE08BA4F5090E6BC3060F42BC7CD15A71EB5B117554AEB395B22E5C2EEA7D0EFC36FF13BEC13B156879B87641505
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\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

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostName.XSL	
SHA-512:	2C25363DCCDB718D427CE451963F1616344A59A57AF0A19F946B7C06536E773E0EA383AC48AAC35E109327B7B86432D608CB0490EBF9590A31AA87330D6F929E
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=

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
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

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\IEEE2006OfficeOnline.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="/">....<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
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

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\MLASeventhEditionOfficeOnline.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($format, 3)" />.....<xsl:with-param name="parameters" select="$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
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):	3.124586952155478
Encrypted:	false
SSDEEP:	768:catNbFeZKdogeyHMOeYhIVi+iOFOqbPXdEmanb:j/eLAhIVJb2
MD5:	186E4573373798AA3A16DA069BCDE57A
SHA1:	8252DC752691D9C2CF2671A7AEF167220FCC2BAA
SHA-256:	E11DB888A385F42784D95BF918467708D7F77557E06BB045A712634316599B55
SHA-512:	F893DD7F9C8EBAB08E4CC6E892A597CA7A5C699DB1DB9C784D06CD73DC7C60DC9EE01D90E1DF006E66FB622875006923053E40A0DAA0BEBBB35352FAFB8C7C6
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\MSO1033.acl	
Preview:	.....y..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\Business Account 395022 Non Taxable.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 14:27:01 2020, mtime=Tue Sep 28 02:47:40 2021, atime=Tue Sep 28 02:47:37 2021, length=67956, window=hide
Category:	dropped
Size (bytes):	2396
Entropy (8bit):	4.732215630018139
Encrypted:	false
SSDEEP:	48:8MwpHeHs1qBBWViB6pMwpHeHs1qBBWViB6:8LpHeHfTWViKLpHeHfTWVi
MD5:	93F8F0743E2075C9A948958BF4421D38
SHA1:	A6BC11C8910191B7CCF2EC1FE613A4C179EDD38E
SHA-256:	B1BBF061BF30A4690B2BBB07362E7814C3B033E4183A4CCCCE9301969F45922F
SHA-512:	F29184A1D1D6842A30DC1D83C505A785ADE0FA13F5A318B1155D32A71B27733C1ABCF4F83B9C1DD1465E36D0CD0858D002CFBD5E738FD38B10D628458BABD79
Malicious:	false
Preview:	L.....F.... .....$>.....Q.....#.....t.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..<S.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....Z.1.....>Qb{..user..B.....N..<S.....S.....v.P.e.n.g.i.n.e.e.r.....~.1.....>Qf{..Desktop.h.....N..<S.....Y.....>.....QI..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.t...<S.. .BUSINE~1.DOC.....>Qa{<S.....R.....g.B.u.s.i.n.e.s.s. .A.c.c.o.u.n.t. .3.9.5.0.2.2. .N.o.n. .T.a.x.a.b.l.e...d.o.c.x.....q.....-.....p.....>.S.....C:\Users\user\Desktop\Business Account 395022 Non Taxable.docx..?.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.B.u.s.i.n.e.s.s. .A.c.c.o.u.n.t. .3.9.5.0.2.2. .N.o.n. .T.a.x.a.b.l.e...d.o.c.x.....:.,.LB.)...A}...`.....X.....932923.....!a..%.H.VZAj...r...1.....-$..!a..%.H.VZAj...r...1.....-$.....1SPS

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=Tue Sep 28 02:47:38 2021, mtime=Tue Sep 28 02:48:42 2021, atime=Tue Sep 28 02:48:42 2021, length=0, window=hide
Category:	dropped
Size (bytes):	1177
Entropy (8bit):	4.695383235743881
Encrypted:	false
SSDEEP:	24:85p00xc30womo9+vA+8buTYa+D77aB6m:85p/CEw9oM4+QuTF+DiB6
MD5:	0667D2C3D14D529169DCCCE360CA3BFD
SHA1:	5B2D011B3CE1C9E381C09E4A3303890CFD8AA435
SHA-256:	5BB2C4C48FA1C07A25599DB654ADC9F29E44317AE6ACE56D331ECB9D456E664A
SHA-512:	D4F524A5AEF0CB309D4E54E0F304F3A39C099513DFDFB25E08CD2DB01E6214D39885562A7D66F5C92CFB0F81CD6A545AACD4CEA020711F1D2A1B1A9501430C6
Malicious:	false
Preview:	L.....F.....8.....TH.....C.....e....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..<S.....:.....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..<S.....S.....v.P.e.n.g.i.n.e.e.r.....V.1.....N....AppData.@.....N..<S.....Y.....t..A.p.p.D.a.t.a.....V.1.....N....Roaming.@.....N..<S.....Y.....D...R.o.a.m.i.n.g.....\.1.....<S....MICROS~1..D.....N..<S.....Y.....f..M.i.c.r.o.s.o.f.t.....\.1.....<S....TEMPLA~1..D.....<S..<S.....<.....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.....932923.....!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):	122
Entropy (8bit):	4.912357990776715
Encrypted:	false
SSDEEP:	3:HsQIRFPdO9yXOMd6lm4nRFPdO9yXOMd6lpnbJlv:HxCF8yeMd63F8yeMd67v
MD5:	86BCAA36DB70A5399B0D9917F66FF2C8
SHA1:	EFE44ADB684164BB53E637867F62E55112E5827F
SHA-256:	FFE62834242D325174B9131DE475008E4DF6845EA08CF2C8E87B1874755AFA2E
SHA-512:	FE01FCFCCC8792A79D1B1D46CE73C19DA92E2125D132EB0BFCDFA572A0568419DA9818D63F13FFA59F68F75455D7D4F287F7B857B451D4042F83490E9BC8A4F
Malicious:	false
Preview:	[misc]..Business Account 395022 Non Taxable.LNK=0..[folders]..Business Account 395022 Non Taxable.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

C:\Users\user\AppData\Roaming\Microsoft\Templates\Normal.dotm (copy)	
Category:	dropped
Size (bytes):	17935
Entropy (8bit):	7.402535788975686
Encrypted:	false
SSDEEP:	384:KaN8PC78Wky1XKP6qECo/6akwLWdxdlpeB1z9rSNR+7V+ij:oQ8Wk3P6qE2akw6LlpeQX+7hj
MD5:	4CD13809C72AD4BC83ECBE975F647A22
SHA1:	5999CAA6341ADE5CA41E7252BC83E9E6655C553F
SHA-256:	8C78603CF759E5D5B69674B636B5BCA05C7FE0B7327ADB8A96206AA3C797BB16
SHA-512:	6FAE83F8931022204A6E914B9B55E3A9139CEC674E40DA578A5D2986D3659A1E9EF891D780E919E27C39E40010DEC8CC6EB1734D305CF90F5D3FD66990D6F87
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...I@.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
Size (bytes):	162
Entropy (8bit):	3.4487877630347388
Encrypted:	false
SSDEEP:	3:Rl/ZdnP9cdnlluhfe94pNSZpnyYDE3o:RtZTcEJe2pNSiW7
MD5:	348E836E7C2ABDC864DD86F5C99786EB
SHA1:	D6F74969F7EFEF3620BA7F8118FDE56EAB73DF21
SHA-256:	DA54F6D847B09F5B69DC11B4BB1ACCCF96190F9F947CDFD5D6811DD3EC13B157
SHA-512:	122DC1B56A09AC23877403BDA7C96799F1A551F52C8E605675420C6A790E48D0B4DDFA0406B513B01BB0611A73988AAC0C78707665F2957C116161BB71ADA6EA
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h...8.....4..x.-....p.r.a.t.e.s.h...8.....8..x....@z..Hr.npz..hr.n.{..hr.n<..x./...}...}.LMEM

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):	17935
Entropy (8bit):	7.402535788975686
Encrypted:	false
SSDEEP:	384:KaN8PC78Wky1XKP6qECo/6akwLWdxdlpeB1z9rSNR+7V+ij:oQ8Wk3P6qE2akw6LlpeQX+7hj
MD5:	4CD13809C72AD4BC83ECBE975F647A22
SHA1:	5999CAA6341ADE5CA41E7252BC83E9E6655C553F
SHA-256:	8C78603CF759E5D5B69674B636B5BCA05C7FE0B7327ADB8A96206AA3C797BB16
SHA-512:	6FAE83F8931022204A6E914B9B55E3A9139CEC674E40DA578A5D2986D3659A1E9EF891D780E919E27C39E40010DEC8CC6EB1734D305CF90F5D3FD66990D6F87
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...I@.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

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Preview:	..

C:\Users\user\Desktop\~$siness Account 395022 Non Taxable.docx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.4487877630347388
Encrypted:	false
SSDEEP:	3:Rl/ZdnP9cdnlluhfe94pNSZpnyYDE3o:RtZTcEJe2pNSiW7
MD5:	348E836E7C2ABDC864DD86F5C99786EB
SHA1:	D6F74969F7EFEF3620BA7F8118FDE56EAB73DF21
SHA-256:	DA54F6D847B09F5B69DC11B4BB1ACCCF96190F9F947CDFD5D6811DD3EC13B157
SHA-512:	122DC1B56A09AC23877403BDA7C96799F1A551F52C8E605675420C6A790E48D0B4DDFA0406B513B01BB0611A73988AAC0C78707665F2957C116161BB71ADA6EA
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h...8.....4..x.-....p.r.a.t.e.s.h...8.....8..x....@z..Hr.npz..hr.n.{..hr.n<..x./....}...}.LMEM

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.906511090259427
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:	Business Account 395022 Non Taxable.docx
File size:	67956
MD5:	ba70eb4f3ca9df379b21709ea09ba5a2
SHA1:	673ef069a308bf237ea47aae92ef5e540ab92be0
SHA256:	e9947191baba0ebbfcbf318d4f527a6d45282be150efa174c770eb7f60792b18
SHA512:	d82fe7504dfdd5320eb5e233a377dd410e87ea34731855 41ab9944cd704b641e6b1cac71f2e2286389bf384a3a9bb ca6f30966391300ec2f6e00a9044768afa
SSDEEP:	1536:NodeN8b6UrX/PJg79A8WJ53cbQj7ZxzgWGJMCAM+BXOnTX:XNq/Pw1WJ53cbqfs1JMCAtBwj
File Content Preview:	PK.....!.i.*f.....[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: 6128 Parent PID: 792

General

Start time:	20:47:37
Start date:	27/09/2021
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:	0x280000
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