ID: 491720
Sample Name: Business Account 395022 Non Taxable.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:41:00
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

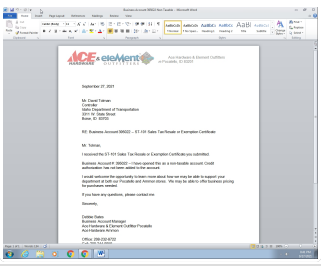
Windows Analysis Report Business Account 395022 No…

Overview

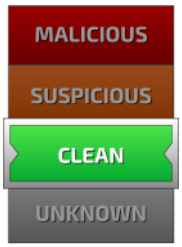
General Information

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

Most interesting Screenshot:



Detection

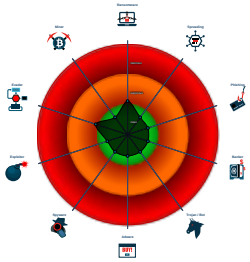


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 284 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

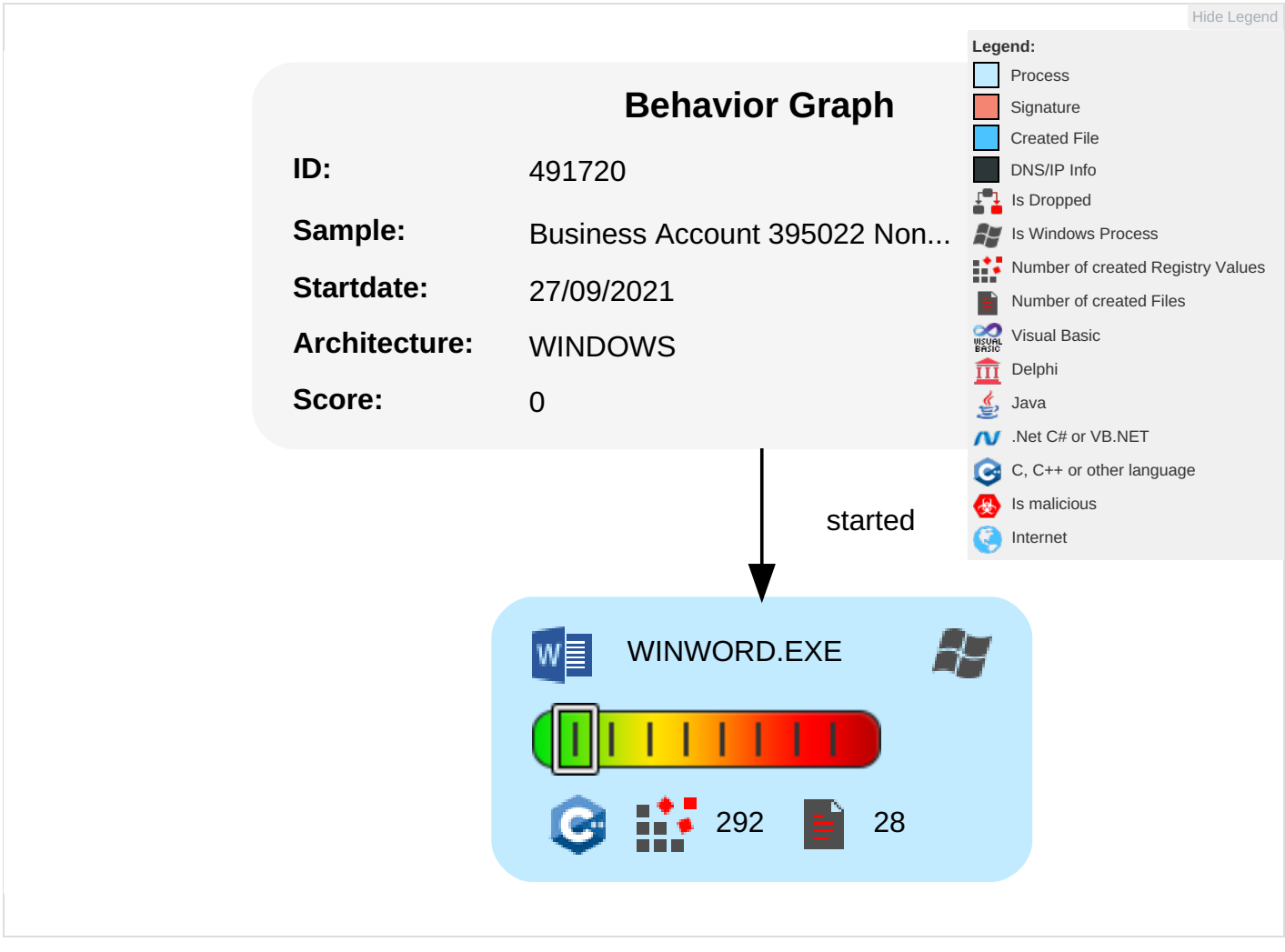
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

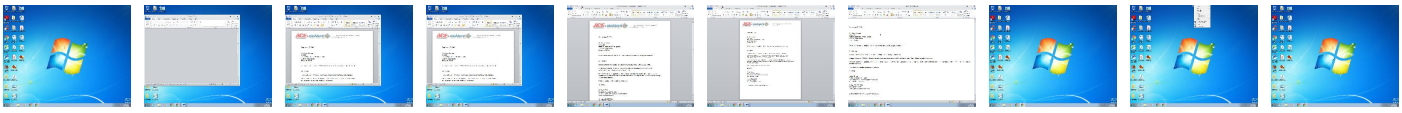
Behavior Graph

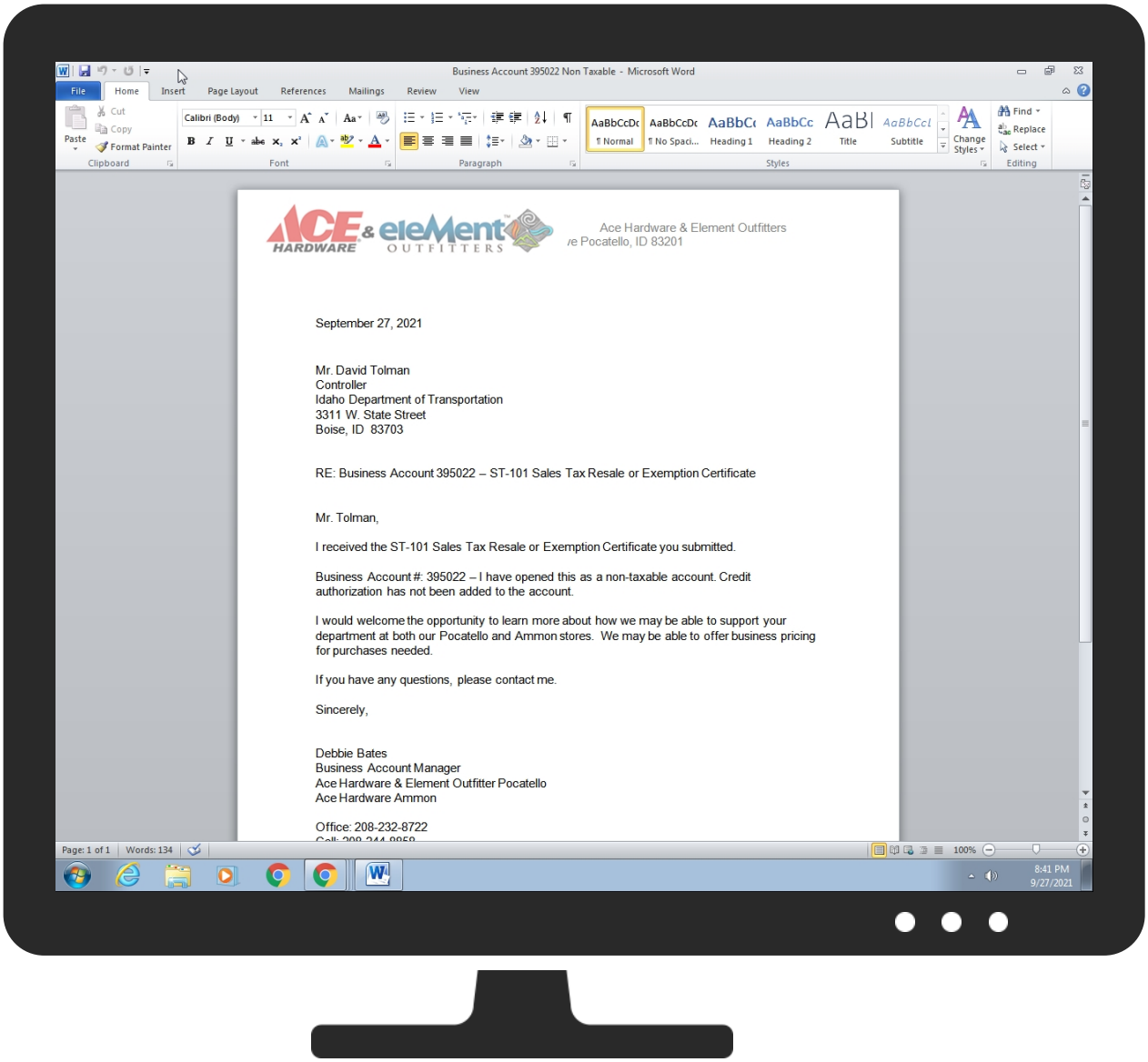


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491720
Start date:	27.09.2021
Start time:	20:41:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 25s
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 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	3
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winDOCX@1/8@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F5FA9C0.png	
Process:	C:\Program Files\Microsoft Office\Office14\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.|.. .)HA.R.....GA.R.... ..gH.|>.^.....=<.../..dw.. .)HA.R.?.....ea!....)S.}.0^..R.... .)HA.IR..O....q...qM....x..'.FA.R.... ..SI.|>.....DW....*x0v,..<.}. .)HA.R.....>.I.....I...+nJ$.RVF..#...eO(HA.R.....*)..GP.gx.d1.[4ET...+U.3>).... .1.S.R.... .).J.....O7oFb.....T...ok....9..^../^.V.... .)HA.DR... .4...#y.@D.+..*.....\|.AT.r....<....g...R.... ...TTT...I./.....^.D.....].,bk}K..b....U. .Je.9;..v.,..#../.?...\|.x..EO.....(HKG Aj..R..sv....=~.....E,...\|.. .)HA..b.s..i.^...7n.k...I...$..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\Temporary Internet Files\Content.Word\~WRS{09A8CC8C-610D-44B3-8B14-98C4F67A79DC}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{43EFE90C-1593-44A8-8EB7-8476100ED0C7}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\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\Office\Recent\Business Account 395022 Non Taxable.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 30 20:09:01 2021, mtime=Mon Aug 30 20:09:01 2021, atime=Tue Sep 28 02:41:21 2021, length=67956, window=hide
Category:	dropped
Size (bytes):	2288
Entropy (8bit):	4.581234472241625
Encrypted:	false
SSDEEP:	48:8iT4/XTUrffBRlRWf2iT4/XTUrffBRlRWB:8Z/XQrnvlRWf2Z/XQrnvlRWB
MD5:	0771EFCE8102F0D1DBA39EA91D5F9CFD
SHA1:	E2C81860F0B19347227BFAA0CCA8780FB97022FE
SHA-256:	BCC4BC03D8C6351FFAA206154460B31642E39DAEED31CE77356BE26B9FE82ADA
SHA-512:	19BC8D6E9D1F7620159EC9288C757CDC853ADB4E1ED7134F1D90DD23DCFCCBECFCEEF0A5AFF858CF4557FF8C245EE87B018505349FA7718CFA740725D901E 75
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....A.....A.....t.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....S"...user.8.....QK.X.S".*...&=....U.....A.l.b.u.s.....z.1.....S#...Desktop.d.....QK.X.S#.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1. 7.6.9.....2.t...<S+. .BUSINE~1.DOC..~.....S!..S!.*.....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.....-...8...[.....?J..... C:\Users\..#.....\\849224\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.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	145
Entropy (8bit):	4.769092577528504
Encrypted:	false
SSDEEP:	3:HsQIRFPdO9yXOMd6l/Q0RFPdO9yXOMd6lmxWsQIRFPdO9yXOMd6lv:HxCF8yeMd6tQOF8yeMd6DCF8yeMd61
MD5:	F42032243B59973A843DAE1A48E370B7
SHA1:	D8D91359233432F910426D8411A2C74771612885
SHA-256:	7C4C4AFDAA54B89186D7167AC3C3838460DEAA73276D416834F6E7C898F518E7
SHA-512:	56E37E678C81A7BE9E91CBB849ABA55082135CA15753F7EBCE6C21058F39323E60996252E3EB4A3EC5CEC7AEEFE506A9FE472D9FD973737991617CDF0AB5C2 E
Malicious:	false
Reputation:	low
Preview:	[misc]..Business Account 395022 Non Taxable.LNK=0..Business Account 395022 Non Taxable.LNK=0..[misc]..Business Account 395022 Non Taxable.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false

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

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~$siness Account 395022 Non Taxable.docx	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyDFH5UKycWT5yAi/lln:vdsCkWtgZ2YAyll
MD5:	6525B5171CE36A6D7EDB3E4DFD5CB579
SHA1:	70AFC3864539BCF8F1C4CD336F6096534A6268FA
SHA-256:	617E1415F4483DAE29072F8E5A042E9EB3446F53F9AC2F26180AECD1D93151CF
SHA-512:	700AEAE11F026EDE01A59B5CC1166D041E1B100E91F84F984D072CDB154251AD15A11C629B8CD7314CB0B2FF8669C3C52EB592020FBA2502CB35BDE6D1EA832
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.906511090259427
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 41ab9944cd704b641e6b1cac71f2e2286389bf384a3a9b ca6f30966391300ec2f6e00a9044768afa

General

SSDEEP:	1536:NodeN8b6UrX/PJg79A8WJ53cbQj7ZxzgWGJMCAM+BXOnTX:XNq/Pw1WJ53cbqfs1JMCAtBwj
File Content Preview:	PK.....!.i.*f.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 284 Parent PID: 596

General

Start time:	20:41:21
Start date:	27/09/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f700000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Disassembly