

JoeSandbox Cloud BASIC



**ID:** 682653

**Sample Name:**

airdynefile08.11.22.doc

**Cookbook:**

defaultwindowsofficecookbook.jbs

**Time:** 19:56:47

**Date:** 11/08/2022

**Version:** 35.0.0 Citrine

# Table of Contents

Table of Contents	2
Windows Analysis Report airdynefile08.11.22.doc	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Signatures	4
Sigma Signatures	4
Snort Signatures	4
Joe Sandbox Signatures	5
AV Detection	5
System Summary	5
Mitre Att&ck Matrix	5
Behavior Graph	5
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	8
Contacted Domains	8
World Map of Contacted IPs	8
Public IPs	8
General Information	8
Warnings	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASNs	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5AD8DEF.png	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5B980826.png	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{A1B0D7EC-F7EF-4F37-9130-CDF90AC285CB}.tmp	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{09291B43-D50C-46A7-AEE5-876A9B012E3A}.tmp	11
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6194CBA3-C75A-48F7-92FA-E05C839B7F47}.tmp	11
C:\Users\user\AppData\Local\Temp\~DF176F4133B71F1140.TMP	11
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\airdynefile08.11.22.LNK	11
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	12
C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm	12
C:\Users\user\AppData\Roaming\Microsoft\UPProof\ExcludeDictionaryEN0409.lex	12
C:\Users\user\Desktop\~\$rdynefile08.11.22.doc	13
Static File Info	13
General	13
File Icon	13
Static OLE Info	13
General	13
OLE File "/opt/package/joesandbox/database/analysis/682653/sample/airdynefile08.11.22.doc"	13
Indicators	13
Streams with VBA	14
VBA File Name: ThisDocument.cls, Stream Size: 2860	14
General	14
VBA Code	14
Streams	14
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365	14
General	14
Stream Path: PROJECTwm, File Type: data, Stream Size: 41	14
General	14
Stream Path: VBA\ VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7	14
General	14
Stream Path: VBA\__SRP_2, File Type: data, Stream Size: 5108	15
General	15
Stream Path: VBA\__SRP_3, File Type: data, Stream Size: 2724	15
General	15
Stream Path: VBA\dir, File Type: data, Stream Size: 486	15
General	15
Network Behavior	15
TCP Packets	15

Statistics

15

System Behavior

16

Analysis Process: WINWORD.EXEPID: 2492, Parent PID: 576

16

General

16

File Activities

16

File Created

16

File Deleted

16

File Read

16

Registry Activities

16

Key Created

16

Key Value Created

17

Key Value Modified

18

Disassembly




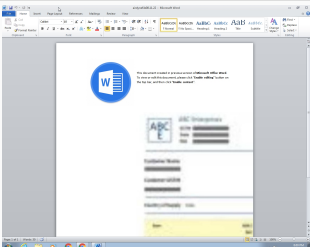
22

# Windows Analysis Report

airdynefile08.11.22.doc

## Overview

### General Information

Sample Name:	airdynefile08.11.22.doc
Analysis ID:	682653
MD5:	9cbf5c3239d290...
SHA1:	e0fab1bc0137f94..
SHA256:	3c59aab375e8eb..
Tags:	<div>doc</div> <div>lcedID</div>
Infos:	<div></div> <div></div>

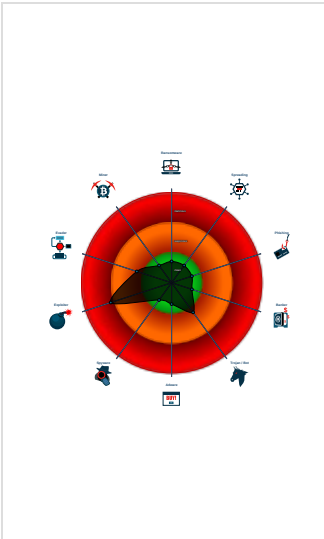
### Detection

<div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div>	
Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%


### Signatures

Multi AV Scanner detection for subm...
Document contains an embedded V...
Machine Learning detection for sam...
Potential document exploit detected...
Tries to connect to HTTP servers, b...
Document contains an embedded V...
Document contains embedded VBA...
IP address seen in connection with ...
Document misses a certain OLE str...

### Classification



## Process Tree

- System is w7x64
-  WINWORD.EXE (PID: 2492 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- cleanup

## Malware Configuration

No configs have been found

## Yara Signatures

No yara matches

## Sigma Signatures

No Sigma rule has matched

## Snort Signatures

No Snort rule has matched

# Joe Sandbox Signatures

## AV Detection



Multi AV Scanner detection for submitted file

Machine Learning detection for sample

## System Summary

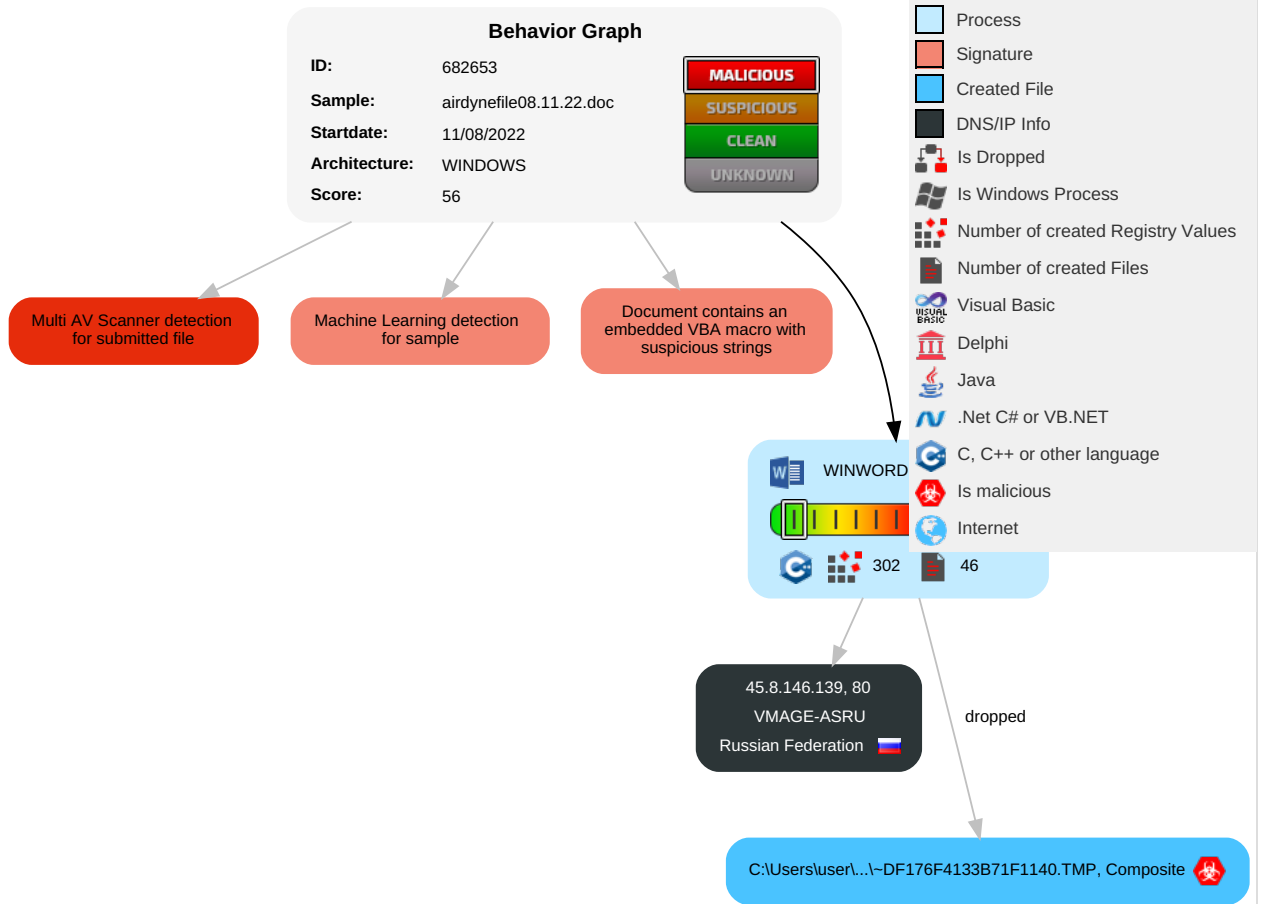


Document contains an embedded VBA macro with suspicious strings

## 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	1 2 Scripting	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 2 Scripting	LSASS Memory	1 System Information Discovery	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

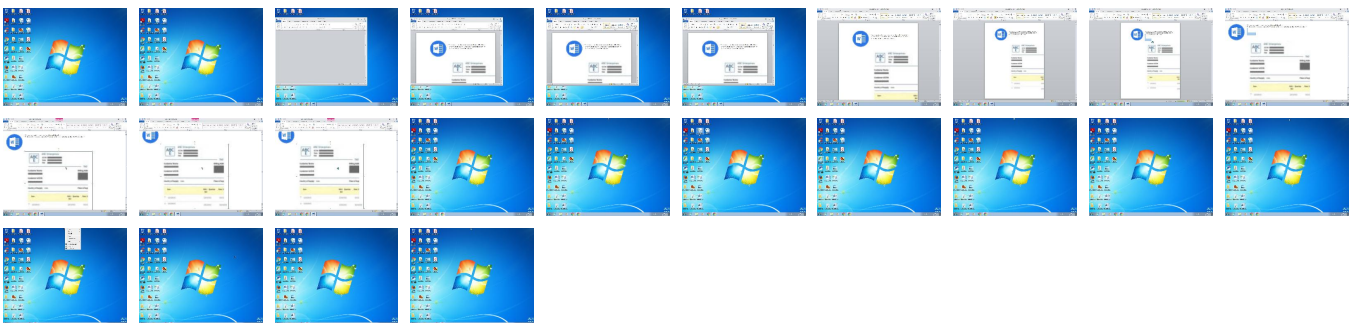
## Behavior Graph

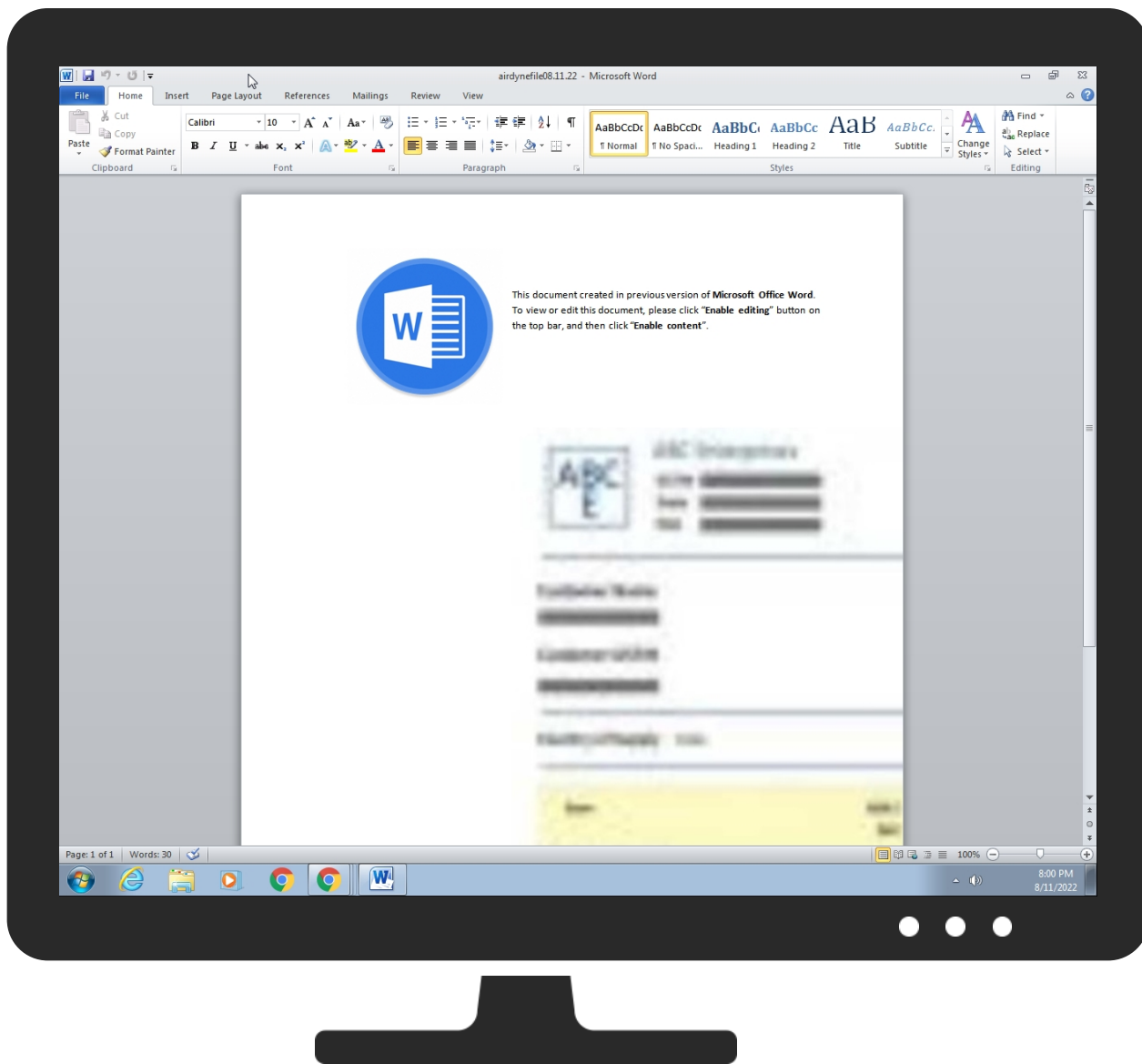


## Screenshots

### 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
airdynefile08.11.22.doc	27%	Virustotal		<a href="#">Browse</a>
airdynefile08.11.22.doc	15%	ReversingLabs	Script-Macro.Trojan.Amp hitryon	
airdynefile08.11.22.doc	100%	Joe Sandbox ML		

### Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF176F4133B71F1140.TMP	100%	Joe Sandbox ML		

### Unpacked PE Files

🚫 No Antivirus matches

### Domains

🚫 No Antivirus matches

### URLs

⊘ No Antivirus matches

## Domains and IPs

### Contacted Domains

⊘ No contacted domains info

### World Map of Contacted IPs



### Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.8.146.139	unknown	Russian Federation		44676	VMAGE-ASRU	false

## General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682653
Start date and time:	2022-08-11 19:56:47 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	airdynefile08.11.22.doc
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:	4
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:	<ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• GSI enabled (VBA)</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.expl.winDOC@1/11@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 100%</li><li>• Number of executed functions: 0</li><li>• Number of non-executed functions: 0</li></ul>
Cookbook Comments:	<ul style="list-style-type: none"><li>• Found application associated with file extension: .doc</li><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Found Word or Excel or PowerPoint or XPS Viewer</li><li>• Attach to Office via COM</li><li>• Scroll down</li><li>• Close Viewer</li></ul>

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe
- Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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\5AD8DEF.png 	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 636 x 613, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	113730
Entropy (8bit):	7.990292786537194
Encrypted:	true
SSDEEP:	3072:ShliMUFV26oUc72DI+oj/Yc6oGqdxVJw0c8N2mirB0VZp:ShMggmEceUi8N2miK/
MD5:	E0B30095BE35E9494E5073277D4FC1A1
SHA1:	19D39B036989A331F5389E377FBE565436599894
SHA-256:	EA952A68D25232D981CDBE0CD6DA947A9386D4BFFD5D1BE2EF80C4A1246AC3E2
SHA-512:	A524907D5D60AA77DB0BA3A3BF114EA7F8AEA9190ADAA84A0C78F96EC8E333AB124D68C84863E83E735D602117B0F3422746C9C4A0D6823CC8B51B652C41977E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR..... .....e.....V.R...IDATx.....4.....~.....t.....\$.....d.....+...%Y.,V.(...7...03""...O.....?>..y.}.v.&u.....?0....g.NH.....F...\$.H.....km.%"D .=:f;.....A....O..w...n...U....N~?".....'...7w)A..l.....7....q .q.7?.....v.f...6....x...<On.WLm.>s<-.....".....".....~a...f=...7....P.~...gD...:P...*.....c...;B...q..1.> ....R.7m...7.....".p7%.M.".....9.P.8.!..?....)".....A.Z.rA.).g.7..'QD.....@\$.....*..oC...6w...lP...lN..1X..H.....q...X{s.A.....w..l...l'..t.C87.p.k...H>r...),...n..Dd.R.c.xHs.nWv.....>.j.WCi...a...}.t _...A.q.t.^A.Q..g...P.h.n.nm...7...YYT.....jl....yR>s...w..... Z..L.....\FP....QG...0....2...@T.*....C....M...;l...Y8...R.Y*....~.;CA.....q...6'.....~.....2.g.".../.{x( ...o.p...YW&+//[.....]...h....s....&..m_)tG...s...<..].R..w..l.....A;.....l..l @...&....0[.la?..`#2upVW.4.{..c.JMZ..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5B980826.png	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 440 x 440, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	255895
Entropy (8bit):	7.979759984902193
Encrypted:	false
SSDEEP:	6144:P5rAVWEVtBoN+zhOdTeH3/kldpFO23BgSD5rPnuV0UJc4:P5jkTB26Olev0T3v9jUJb
MD5:	9B32A04B89F73BF2C6DB5756158B35B5
SHA1:	3389E751C09D18696F2BCD1C54E8AA5931066760
SHA-256:	337CA9401C94826508B2E027E35C63D60B05821AEFF587388E6F11A2B12ADA0A
SHA-512:	A14901247DE770DCEDAB27DA1A05A9F11B588396C78E8405F2BDC6421B80F8CA1C5F61DA629F62B83489E63DF2BC74E11B36A49F05096FE60DD038A1E2DDD F
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs..!.....IDATx^....fEu;...7.....7.V[L0&11dTo4...4.qLL4...b;!(" .4...`4.....W..D.....>C...G...<...[{..E..4...PJUk.Z5.]kU...>.(...W.K.z.z2lC.E.....cr.W.Yg.T9...-g..u.h."eZ...W.....w.A..O.5..r.Un.Y.....V..4.NZ....L.HT^+.....\..+..e>..^ ..... "e.m)cHyP.....o.\$Zz..r...?.[T~]/..{2-.m#.?..Uz...p.r...H~SA..HS&.Z.D['.bE&w.'/.Hzv...Z...5...\.l.vPk..l'i/-.=Z. ...O.4.r.6.j.Y...n.n.6.q. ....]}?@::;T...m....j.5]... .....'Z..g..Zw.z"...[...:ZT~+...0..V..oy.....O...1.U...m..Kz.....L...8.2=1...oeW=..s.{t0F....M.!y..j l.zf..2l....L.....h....%z..4q..._eZ^..W^...m..d..3.b....i...T.....k.R..J..V.o..+o.....'....+.*'...g...z-{HZ...j~.....mh1&.3.....D..}.cPiU&M...m... .e...B...B.g..@..Plo...s..1]..+.MW9Pi.x..m..U>...z...oc...6..^H.4....L.U...l{.....*z.*_..6.r.g.5]1...1:.....5....c.{l.l.J..D..^1.d{...}Se3.-?.,\$.'{B<O....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{A1B0D7EC-F7EF-4F37-9130-CDF90AC285CB}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.700244852937293
Encrypted:	false
SSDEEP:	96:7DAKt/Zt0XCP9hMbP9UD54vvfcnnE2lt9aB2iot/ZxiO0Xb9XhMbP9UD54vvfcB:7kKtEc/c04vvEEkastkb/c04vvEEka
MD5:	ACF4A546564A09955106D0E56DBD06F6
SHA1:	8D319FB5252FE8A583695B3B9D5BAB41DFDD7A96
SHA-256:	B683B00E78D30F27256BF2FFA58516CA7D0FBD22294C5AF89EDF7FAEB4240813
SHA-512:	4890C8F3FF4C5DF019F70D88EBEC8A4EA14BA7E36DBCAFAD95D45B2C0266C110D56F09CB64027C87C452842E98169A38AB8BB476D0AAAF7179956D3B3A8B98477
Malicious:	false
Reputation:	low
Preview:	.....>..... ..... ..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{09291B43-D50C-46A7-AEE5-876A9B012E3A}.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:	95F83AE84CAFCCEDE5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..... ..... ..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6194CBA3-C75A-48F7-92FA-E05C839B7F47}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.1363686128594344
Encrypted:	false
SSDEEP:	12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82lkYkwkvLK4Z9e4Cne4PllleHkUZw/W4c:4LG1ND9Pxn82yYkNKYEOYyHXz
MD5:	EC84F2FF891EC42BBD816CF344411B04
SHA1:	0B451B44709F2D8F1B4EB2F418EE6A498E437F5A
SHA-256:	3DD13A2A6C1ACC9D4E0EC56C77F4DB65CEBF47836C5AFA0CC781C00569CDE158
SHA-512:	56E9951C7C4C139B4F4A930A205653D7451A4915555F3D8883B095B5B1BCBA14729E13DB3B62956A581FB3E77C3F17533C8FB3382DBC972ADB60D6F66911304A
Malicious:	false
Reputation:	low
Preview:	./././...T.h.i.s..d.o.c.u.m.e.n.t..c.r.e.a.t.e.d..i.n..p.r.e.v.i.o.u.s..v.e.r.s.i.o.n..o.f..M.i.c.r.o.s.o.f.t..O.f.f.i.c.e..W.o.r.d.....T.o..v.i.e.w..o.r..e.d.i.t..t.h.i.s..d.o.c.u.m.e.n.t.,..p.l. e.a.s.e..c.l.i.c.k..E.n.a.b.l.e..e.d.i.t.i.n.g..b.u.t.t.o.n..o.n..t.h.e..t.o.p..b.a.r.,..a.n.d..t.h.e.n..c.l.i.c.k..E.n.a.b.l.e..c.o.n.t.e.n.t.. ..... .....Z..... ..... .....

C:\Users\user\AppData\Local\Temp\~DF176F4133B71F1140.TMP  	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	60928
Entropy (8bit):	4.172177194645338
Encrypted:	false
SSDEEP:	768:u5Uzo0VkhF7l1LdXL90M1uW2OqzN9eBVC9WWGviPLMZoHsGDaq:Y0Vkh9l1LdXL90Mj2dP9vGqz3MGDaq
MD5:	3E74139C6FFBC46694E653125FFB44CD
SHA1:	6C6DA74C286C6B5F64F6883941923F0E3BC18795
SHA-256:	9D1554C12D34D2B3C5F31607D316BB4DD79D757A853E231B439C14D69116A968
SHA-512:	02487840A1BAB44639AF0CCFB7C425E98DF5121E0E4F948BE6B039592973C2E9020EC8A43846CB5C59E837C937DBE79F67E679510F3FA245D2887E09A3CC8EA
Malicious:	true
Antivirus:	<ul style="list-style-type: none"><li>Antivirus: Joe Sandbox ML, Detection: 100%</li></ul>
Reputation:	low
Preview:	.....>..... ..... .....T.....( .....!...".#...\$...%...&...'.....)*...+...-.../...0...1...2...3...4...5...6...7...8...9...:.....<...=...>?...?...@...!...B...C...D... ..E...F...G...H...;...J...K...L...M...N...O...P...Q...R...S...;...V...W...X...Y...Z...^..._...`.....j.....b...c...d...e...f...g...h...[...k...l...u...n...o...p...q...r...s...t..._.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\airdynefile08.11.22.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=Tue Mar 8 15:45:56 2022, mtime=Tue Mar 8 15:45:56 2022, atime=Fri Aug 12 01:59:15 2022, length=2255369, window=hide
Category:	dropped
Size (bytes):	1059
Entropy (8bit):	4.578161638390088
Encrypted:	false
SSDEEP:	12:8x6YEjgXg/XAICPCHaXNBQIB/SxXX+WhyMGhWY5ia7juicvbl8G4wffQVxDtZ3Ye:8xVa/XT9SU8WZoNeCSkDv3qEwu7D
MD5:	9F664585C6748F0C3D96BD33A166FEC6
SHA1:	65180FCEDEBF449DC799E1FB182A8068BD9335EA
SHA-256:	A4940FE0EA4F822B7DCAED064A961FC011904264B1E015DF1F43787B2B6D0189
SHA-512:	2E84240CACFD8E858C7F80A8256ECD968DB0B5593CF88B2046C2B688892C361808F4D332A4E741AE3128655F2857F7529243F3014D2F7C0A395F580BB2350B4B
Malicious:	false
Reputation:	low
Preview:	L.....F.....?...3...?...3...C.....j".....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.....hT....user.8.....QK.XhT.*...&=...U.....A.l.b.u.s.....z.1.....hT....Desktop.d.....QK.XhT.*..._-=.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-2.1.7.6.9.....x.2..j".Uh. .AIRDYN~1.DOC..\.....hT..hT.*...f.....a.i.r.d.y.n.e.f.i.l.e.0.8...1.1...2.2...d.o.c.....8...[.....?J.....C:\Users\.#.....\226533\Users.user\Desktop\airdynefile08.11.22.doc.....\.....\.....\D.e.s.k.t.o.p.\a.i.r.d.y.n.e.f.i.l.e.0.8...1.1...2.2...d.o.c.....,LB.)...Ag.....1SPS.XF.L8C....&m.m.....-S.-.1.-5.-2.1.-9.6.6.7.7.1.3.1.5.-3.0.1.9.4.0.5.6.3.7.-3.6.7.3.3.6.4.7.7.-1.0.0.6.....`.....X.....226533.....D_...3N.

<b>C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	89
Entropy (8bit):	4.66206935403088
Encrypted:	false
SSDEEP:	3:bDuMJlcMRXlwdRjbUmX1rlwdRjbUv:bC1wfjbbwwfjb2
MD5:	768F6BDC43FCB0CE423AE169D54AB0FD
SHA1:	42B20BEA79CB7F30BA795B0F8D3DF6C7E76C54F2
SHA-256:	EA16E2892845962864B4F9AFB78244BC7180B5D322293359A682E8C5854E3615
SHA-512:	C738FA5E9CFE102852F658A960797D207B286246950941B71FB7F104263DE6C5B36A1B697450F43AEDDEB1F9CD204FBC78F4F17BF07555DF5DED1371DCA649AD
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..airdynefile08.11.22.LNK=0..[doc]..airdynefile08.11.22.LNK=0..

<b>C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdl:n:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F052655
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

<b>C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex</b>	
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:	F3B25701FE362EC84616A93A445CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~\$rdynefile08.11.22.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdlN:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265:5
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

Static File Info	
General	
File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993763586131025
TrID:	<ul style="list-style-type: none"><li>Word Microsoft Office Open XML Format document (49504/1) 49.01%</li><li>Word Microsoft Office Open XML Format document (43504/1) 43.07%</li><li>ZIP compressed archive (8000/1) 7.92%</li></ul>
File name:	airdynefile08.11.22.doc
File size:	2349614
MD5:	9cbf5c3239d290b08ba1f0d8617b6802
SHA1:	e0fab1bc0137f946134c22f27bd9f1bb9484c785
SHA256:	3c59aab375e8ebf7a3da914e7f1f38c6c54947b4c27c73c5c591ab27152dfe4d
SHA512:	8042fb552648d95ef3fd785e0d3c2b9efdcdb62ec81012e6d3369e923425948cebed2fc9b4fd165170319f9253bf46156eccfe3822d6959d892dd44725e17b3c
SSDEEP:	49152:QsbTwbt983aPk2JHFeqvFopJNWqsMxhAyiMuBBcRVOI/9wE:IMYkvs7bx0yQWBO45
TLSH:	5FB5330906A1A68F4D64F430376A5B187E612FFB17859F0AA3061D7DE1FDB637A0F0A4
File Content Preview:	PK.....!.U~.....rels/.rels...J.@.....4.E..D.....\$.T..w-.j..... zs..z.z.*X.%(v.....6O.{PI.....`S__x.C..CR.....t.R.....hl.3..H.Q..*.;.=.y... n.....yo.....[vrf..A..6..3[>_...-K....\NH!....<.r...E.B..P...<_.

File Icon	
	
Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info	
General	
Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/682653/sample/airdynefile08.11.22.doc"	
Indicators	
Has Summary Info:	
Application Name:	

Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	True

<b>Streams with VBA</b>	
<b>VBA File Name: ThisDocument.cls, Stream Size: 2860</b>	
<b>General</b>	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2860
Data ASCII:	..Attribute VB_Name = "ThisDocument"...Bas..1Normal...VGlobal!.Spac.IfFalse.JCreatabl..Predeclared..#True."Expose..TemplateDeriv.\$CustomLizC.P....D.?PtrSafeFunction 8....Lib "kernel32" Alias "VirtualProtect" (ByVal ... As Long.8,
Data Raw:	01 ba b4 00 41 74 74 72 69 62 75 74 00 65 20 56 42 5f 4e 61 6d 00 65 20 3d 20 22 54 68 69 00 73 44 6f 63 75 6d 65 6e 10 74 22 0d 0a 0a 8c 42 61 73 01 02 8c 31 4e 6f 72 6d 61 6c 02 2e 19 56 47 6c 6f 62 61 6c 21 01 aa 53 70 61 63 01 6c 46 61 08 6c 73 65 0c 4a 43 72 65 61 10 74 61 62 6c 15 1f 50 72 65 20 64 65 63 6c 61 00 06 49 64 11 00 23 54 72 75 0d 22 45 78 70 08 6f 73 65 14 1c 54

<b>VBA Code</b>

<b>Streams</b>	
<b>Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365</b>	
<b>General</b>	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	365
Entropy:	5.268842495589465
Base64 Encoded:	True
Data ASCII:	ID="{09503B1F-A28D-468B-95E9-CF26489DF7A5}"..Document=ThisDocument/&H00000000..Name="Project"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="ACAE5E0CA6BCAABCAABCAABCAA"..DPB="585AAA4DAB4DAB4D"..GC="0406F6540E010F010FFE"....[Host Extension Info]..
Data Raw:	49 44 3d 22 7b 30 39 35 30 33 42 31 46 2d 41 32 38 44 2d 34 36 38 42 2d 39 35 45 39 2d 43 46 32 36 34 38 39 44 46 37 41 35 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

<b>Stream Path: PROJECTwm, File Type: data, Stream Size: 41</b>	
<b>General</b>	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.0773844850752607
Base64 Encoded:	False
Data ASCII:	ThisDocument.T.h.i.s.D.o.c.u.m.e.n.t.....
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

<b>Stream Path: VBA/_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7</b>	
<b>General</b>	
Stream Path:	VBA/_VBA_PROJECT
File Type:	ISO-8859 text, with no line terminators
Stream Size:	7
Entropy:	1.8423709931771088
Base64 Encoded:	False
Data ASCII:	a . . .
Data Raw:	cc 61 ff ff 00 00 00



# System Behavior

**Analysis Process: WINWORD.EXE** PID: 2492, Parent PID: 576

## General

Target ID:	1
Start time:	19:59:17
Start date:	11/08/2022
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:	0x13fcf0000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

## File Activities

### File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory   synchronize	device	directory file   synchronous io non alert   open for backup ident   open reparse point	success or wait	1	6E0B2B14	CreateDirectoryA

### File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF176F4133B71F1140.TMP	success or wait	1	6E130648	unknown
C:\Users\user\Desktop\~\$rdynfile08.11.22.doc	success or wait	1	6E130648	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
---------------	---------------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

### File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Fonts\StaticCache.dat	unknown	60	success or wait	1	6E42A0EB	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	6E021925	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	6E021925	unknown
C:\Program Files\Microsoft Office\Office14\PROOF\MSSP7EN.dub	unknown	4866	success or wait	1	7FEE916E8B7	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	1	success or wait	1	7FEE9160793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	4096	success or wait	1	7FEE91CAD58	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE9160793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE91CAD58	ReadFile
C:\Users\user\Desktop\lairdynfile08.11.22.doc	1871651	184	success or wait	2	6E130648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5B980826.png	0	65536	success or wait	4	6E130648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5AD8DEF.png	0	65536	success or wait	2	6E130648	unknown

## Registry Activities

### Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E10A5E3	RegCreateKeyExA







Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400100000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358626865	1426784306	success or wait	1	6E021925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400100000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784306	1426784307	success or wait	1	6E021925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784286	1426784287	success or wait	1	6E021925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784287	1426784288	success or wait	1	6E021925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426784286	1426784287	success or wait	1	6E021925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426784287	1426784288	success or wait	1	6E021925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400100000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784307	1426784308	success or wait	1	6E021925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400100000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784308	1426784309	success or wait	1	6E021925	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\7A303	7A303	binary	04 00 00 00 BC 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00	04 00 00 00 BC 09 00 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 54 00 65 00 6D 00 70	success or wait	1	6E130648	unknown





Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
				00 FF FF FF				
				FF				

FF

## Disassembly

 No disassembly