ID: 682653
Sample Name:
airdynefile08.11.22.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:13:16
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

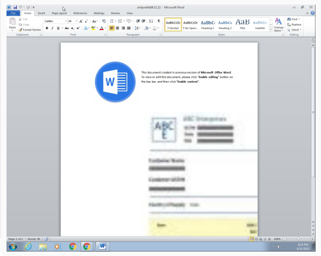
Windows Analysis Report

airdynefile08.11.22.doc

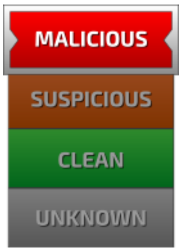
Overview

General Information

Sample Name:	airdynefile08.11.22.doc
Analysis ID:	682653
MD5:	9cbf5c3239d290...
SHA1:	e0fab1bc0137f94..
SHA256:	3c59aab375e8eb..
Tags:	doc IcedID
Infos:	



Detection

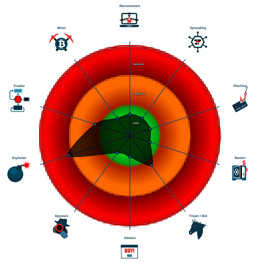


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince v…
- 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: 204 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

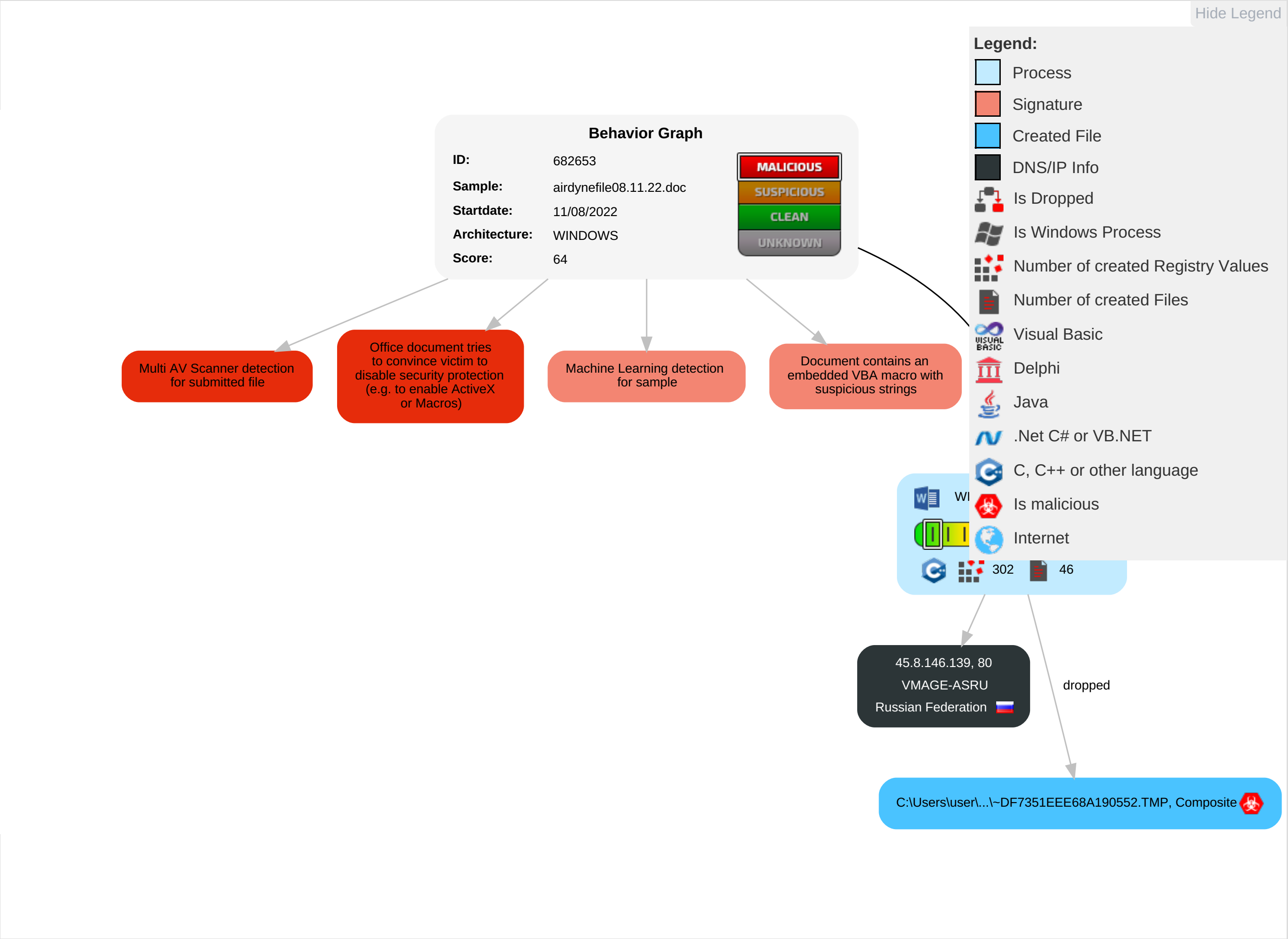
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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 Disable or Modify Tools	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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 2 Scripting	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Behavior Graph



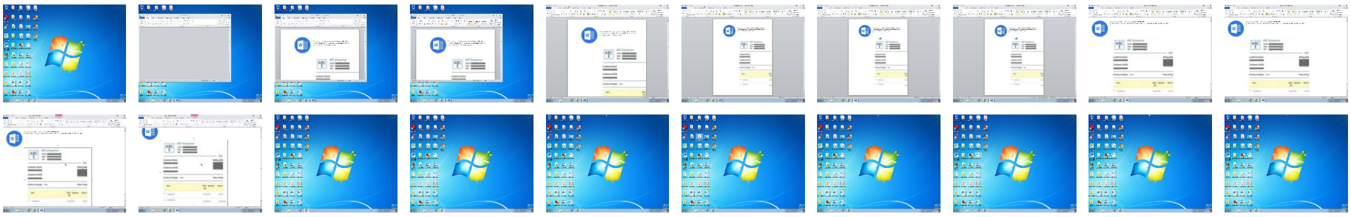
Hide Legend
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet
Behavior Graph
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Multi AV Scanner detection for submitted file
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
Machine Learning detection for sample
Document contains an embedded VBA macro with suspicious strings
WI
302
46
45.8.146.139, 80
VMAGE-ASRU
Russian Federation
dropped
C:\Users\user\...\~DF7351EEE68A190552.TMP, Composite

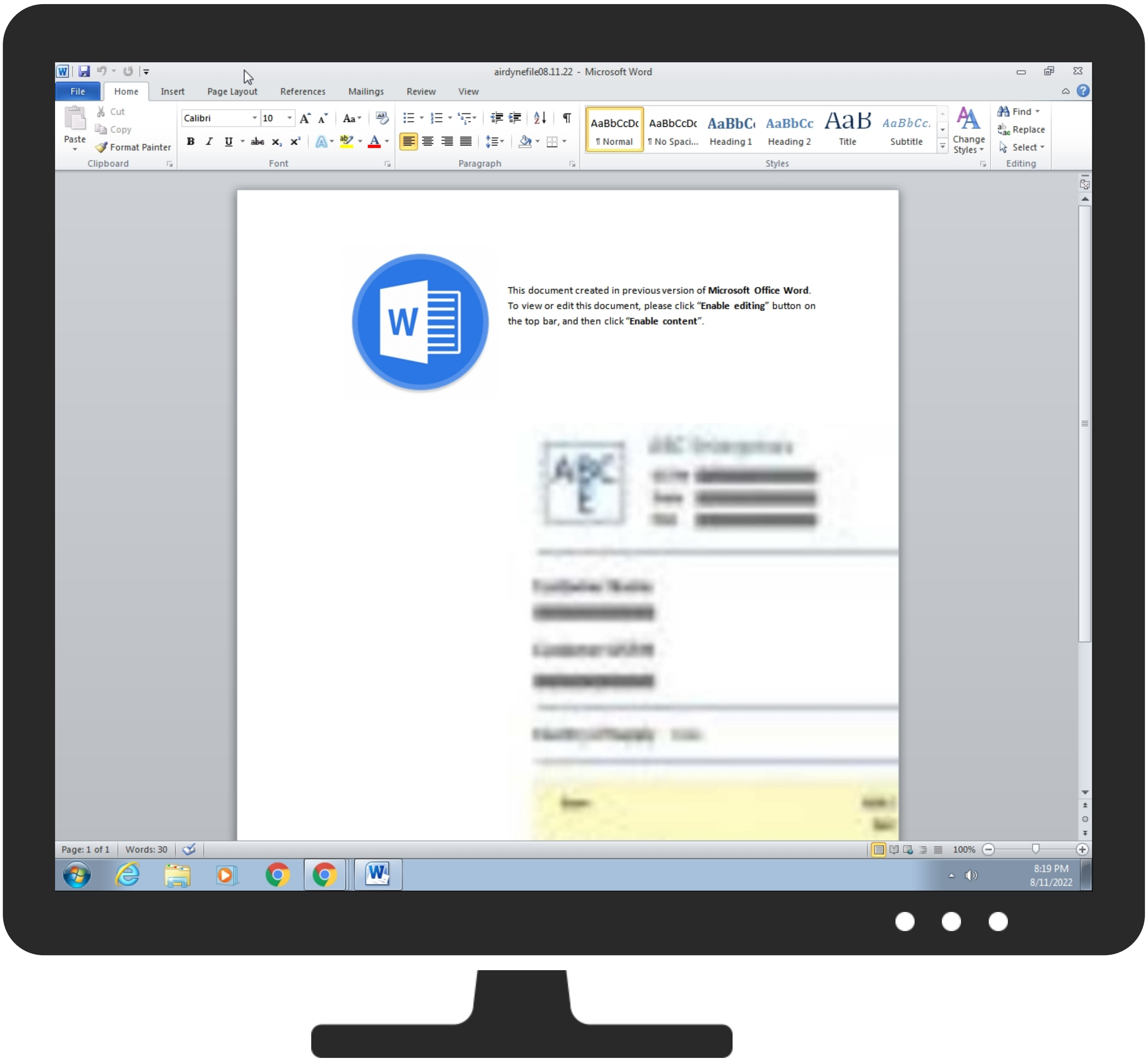
ID:	682653
Sample:	airdynefile08.11.22.doc
Startdate:	11/08/2022
Architecture:	WINDOWS
Score:	64

Screenshots

Thumbnails

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





This document created in previous version of **Microsoft Office Word**. To view or edit this document, please click "**Enable editing**" button on the top bar, and then click "**Enable content**".

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
airdynefile08.11.22.doc	27%	Virustotal		Browse
airdynefile08.11.22.doc	15%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
airdynefile08.11.22.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF7351EEE68A190552.TMP	100%	Joe Sandbox ML		

Unpacked PE Files

⊘ **No Antivirus matches**

Domains

⊘ **No Antivirus matches**

URLs

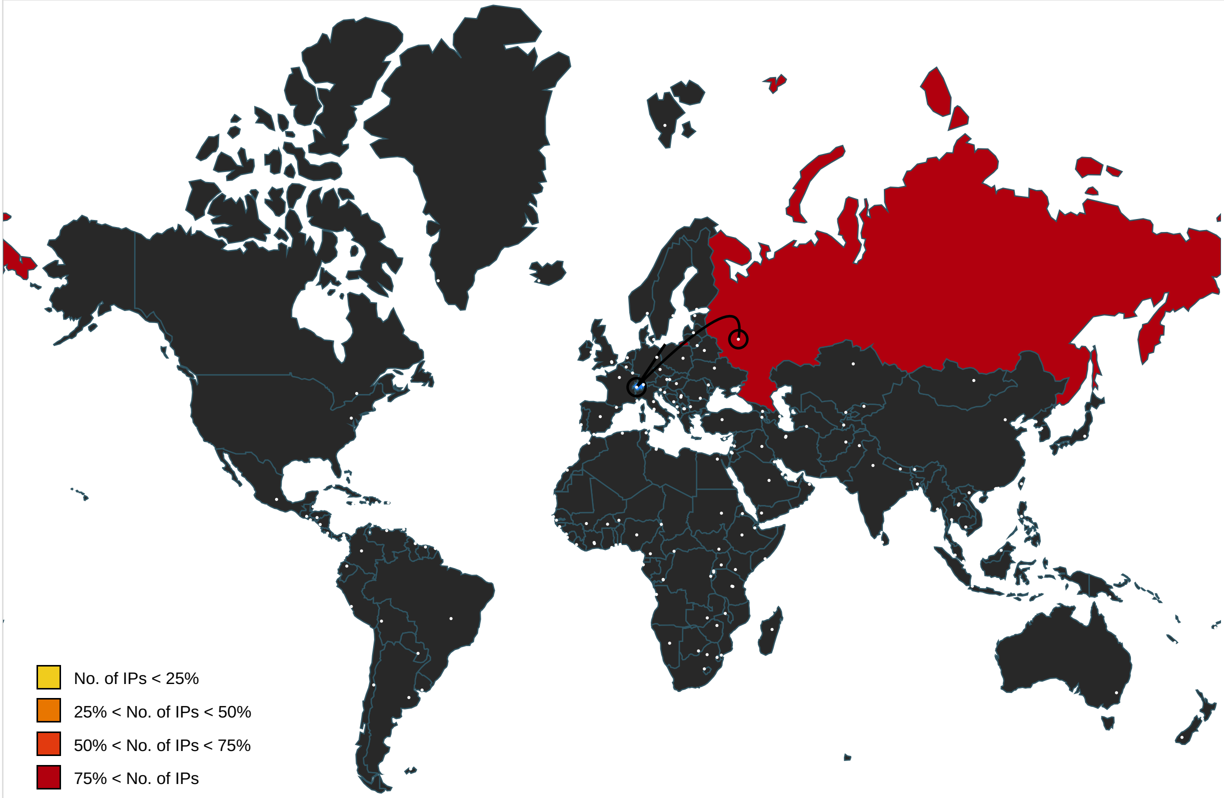
⊘ No Antivirus matches

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 20:13:16 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 30s
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)
Run name:	Without Instrumentation
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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.expl.winDOC@1/11@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

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\1A8EAF99.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:	A14901247DE770DCEDAB27DA14A05A9F11B588396C78E8405F2BDC6421B80F8CA1C5F61DA629F62B83489E63DF2BC74E11B36A49F05096FE60DD038A1E2DDD 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... P]Uk.Z5.]kU...>.(...W.K.z.z2IC.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.$Zz..r...,?..[T~/]..{2-..m #.?...Uz...p.r...H~-SA..HS&..Z.D[.'.bE&.w.`/.Hzv...Z...5..\..I.vPk..l"i-/.=Z.\|....O.4.r.6.j..Y.. ...n.6.q. ....]?@:...;.T...m....:j.5]...\|........'Z..g..Zw.z"....[...:ZT~+...0..V..oy......O...1 .U...m..Kz.....L...8.2-=1...oeW.=..s.{t0F....M.!.y..j\.I.zf..2I....L........h....%z..4q....-_eZ^..W^....m..d..3.b.....i...T......k.R..J..V.o..+o,.....'....+.*.'...g...z-{Hz...j~.....mh1&.3.........D..}.. cPiU&.M...m..,.\|.e...B...B.g..@..PIo....s..1]..+.MW9Pi.x..m..U>...'z...oc...6..^H.4.....L.U....l{......*z.*_..6.r..g.5]1...1:.....5.....c.{.I.!..J..D..^.1.d{:..)Se3.-?.,$.'{8<0.O....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5926E0C6.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:ShIiMUFV26oUc72Dl+oj/Yc6oGqdxVJw0c8N2mirB0VZp:ShMggmEceUi8N2miK/
MD5:	E0B30095BE35E9494E5073277D4FC1A1
SHA1:	19D39B036989A331F5389E377FBE565436599894
SHA-256:	EA952A68D25232D981CDBE0CD6DA947A9386D4BFFD5D1BE2EF80C4A1246AC3E2
SHA-512:	A524907D5D60AA77DB0BA3A3BF114EA7F8AEA9190ADAA84A0C78F96EC8E333AB124D68C84863E83E735D602117B0F3422746C9C4A0D6823CC8B51B652C4197 E
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..I....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...;...i....Y8...R.Y*....~.;.CA........q....6`......~......2.g."... ../..{x.(...o..p...YW&+//[...........]....h....s....&...m_.)tG...s....<...].R..w..!.....A;.....I.,\.I@...&.....0[.\a?..`.#2upVW.4.{..c.JMZ..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{039668B3-0D28-4D8F-8B75-1E6861868320}.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):	28672
Entropy (8bit):	4.051833504731994
Encrypted:	false
SSDEEP:	384:StlgtJq6OaXY9siuBA/c/nEEWtSgtJq6OaXY9siuBA/c/nEE:yoqTN9eBkIECoqTN9eBkIE
MD5:	5FCDA30303B455E44102FF6D5A6CB44C
SHA1:	D3A20755F5CE186A57BB582D4F071ECA7D1A8344
SHA-256:	1E3DD01822B62BF4E3A65C38E9F4E74C47E62A4093D95A1ACDD6374E60362CEE
SHA-512:	37451295529FB325503C92DA526F29B2EEA1326669EE8BAB23CD1764793F0B692F3A6368815AAE315E156A8C160119B29D4FF083545C6E277F1D445375A4FAFE
Malicious:	false
Reputation:	low
Preview:	......................>..(.. ....4...)...*...+...,...-......./...0...1...2...3...5...6.. ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{63A73201-5AE3-4EC8-9715-CBAEE80B9694}.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\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A6354BE5-6BEC-4DC5-B68E-5FC4D17D9101}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF7351EEE68A190552.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):	4.171687721915443
Encrypted:	false
SSDEEP:	768:V5UzoRVkhF7I1Ld9c9qiYuFWOqzN9eBIU9WxGv5ioZoHpGDa4:BRVkh9I1Ld9c9qidWdi9EGM7JGDa4
MD5:	313912C2A47FBD6B6C5DA87494E426D5
SHA1:	4EC39D561EEDC17CC72D2B8DC1D0A0D5F46D1449
SHA-256:	F6AB5F1553072F8728869164B8066028EC84E93D828C82AA0DB90745E8AF1F6B
SHA-512:	B229808E8CEEFDCC3E5CDD7556EE82532C64C48BD0829C710CB2BF3BFC4D548CECFA76F532FEE5D77B91194E7B5446FDC1CD18818FE0E9A01185600347A2D E0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.....................>... ....T...........(............ ....!..."...#...$...%...&...'.......)...*...+...,...-......./...0...1...2...3...4...5...6...7...8...9...:.......<...=...>...?...@...I...B...C...D. ..E...F...G...H...;...J...K...L...M...N...O...P...Q...R...S.......i...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 02:18:17 2022, length=2349614, window=hide
Category:	dropped

Size (bytes):	1059
Entropy (8bit):	4.571455533445305
Encrypted:	false
SSDEEP:	12:896jvjgXg/XAlCPCHaXNBQtB/SxXX+W4hWY5ia7juicvbCfG4wfjQVxDtZ3YilMQ:89A/XT9SUUWZoNeWfSkDv3qNu7D
MD5:	EA9FCF2A71C18E6105218A8742710FE9
SHA1:	253BE37DB4C49B13C509F2C99A23A1DE43907D93
SHA-256:	2369FCFEA88678F4AB2D10439F2538E4DA513DAD71788D31DF38BBAD623DC4AA
SHA-512:	245A125CDA10C1EFBF20282809D92790545CE4ABAD1B8AAE1C524BFA4533FE83486628C3CAA7C8FB2176A270282F59340D49FC8BA61A3406AB4B1C24FFC3E9 7
Malicious:	false
Preview:	L..................F.... ....3.......3....V*......#..........................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...#..UI. .AIRDYN~1.DOC..\......hT..hT..*...r.....'..............a.i.r.d.y.n.e.f.i.l.e.0.8...1.1...2.2...d.o.c......................-...8...[............?J......C:\Users\..#.................. \\536720\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.......536720..........D_....3N.

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):	89
Entropy (8bit):	4.66206935403088
Encrypted:	false
SSDEEP:	3:bDuMJlcMRXIwdRjbUmX1rIwdRjbUv:bC1wfjbwwfjb2
MD5:	768F6BDC43FCB0CE423AE169D54AB0FD
SHA1:	42B20BEA79CB7F30BA795B0F8D3DF6C7E76C54F2
SHA-256:	EA16E2892845962864B4F9AFB78244BC7180B5D322293359A682E8C5854E3615
SHA-512:	C738FA5E9CFE102852F658A960797D207B286246950941B71FB7F104263DE6C5B36A1B697450F43AEDDEB1F9CD204FBC78F4F17BF07555DF5DED1371DCA649A D
Malicious:	false
Preview:	[folders]..Templates.LNK=0..airdynefile08.11.22.LNK=0..[doc]..airdynefile08.11.22.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):	2.503835550707525
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...

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 4

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:	• 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:	airdynefile08.11.22.doc
File size:	2349614
MD5:	9cbf5c3239d290b08ba1f0d8617b6802
SHA1:	e0fab1bc0137f946134c22f27bd9f1bb9484c785
SHA256:	3c59aab375e8ebf7a3da914e7f1f38c6c54947b4c27c73c5c591ab27152dfe4d
SHA512:	8042fb552648d95ef3fd785e0d3c2b9efdcdb62ec81012e6d3369e923425948cebed2fc9b4fd165170319f9253bf46156eccfe3822d6959d892dd44725e17b3c
SSDEEP:	49152:QSbTwbt983aPk2JHFeqvFOpJNWqsMxhAyjMuBBcRVOl/9wE:lMYkvs7bx0yQWBO45
TLSH:	5FB5330906A1A68F4D64F430376A5B187E612FFB17859F0AA3061D7DE1FDB637A0F0A4
File Content Preview:	PK..........!..U~............._rels/.rels...J.@............4.E..D.....$....T..w-..j........|.zs..z..z.*X.%(v......6O.{Pl........`S__._x .C..CR....:....t..R......hI.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

Streams with VBA

VBA File Name: ThisDocument.cls, Stream Size: 2860

General

Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2860
Data ASCII:	..Attribut.e VB_Nam.e = "Thi.sDocumen.t"...Bas..1Normal...VGlobal!.Spac.lFa.lse.JCrea.tabl..Pre decla..Id..#Tru."Exp.ose..Temp.lateDeri.v.$CustomlizC.P.... .D.? PtrSa.fe Funct.ion 8.....L.ib "kern.el32" Al.ias "Vir.tualProt.ect" (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

VBA Code

Streams

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365

General

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 Extender 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 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

Stream Path: PROJECTwm, File Type: data, Stream Size: 41

General

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

Stream Path: VBA/_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7

General

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

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 5108

General

Stream Path:	VBA/__SRP_2
File Type:	data

General	
Stream Size:	5108
Entropy:	1.9217258555644907
Base64 Encoded:	False
Data ASCII:	rU@...............@.......@...............8..............................P..........."...............q.......... ....A..............`..........................................`)......................... ....
Data Raw:	72 55 40 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 22 00 1f 00 00 00 00 00 01 00 01 00 00 00 01 00 71 07 00 00 00 00 00 00 00 00 00 00 a1 07 00 00 00 00 00 00 00 00 00 00 d1 07

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 2724

General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	2724
Entropy:	2.708973861727282
Base64 Encoded:	False
Data ASCII:	rU@...............@.......@......................................x.....`..............p.................A....... ....................................Q.P............0..p......!..........q....................`.q...........\\..p.... ....
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 60 00 d1 08 00 00 00 00 00 00 00 00 00 00 00 00 04 70 10 00 fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 486

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	486
Entropy:	6.288212539715818
Base64 Encoded:	True
Data ASCII:	..........0.... ..H...........Project.Q.(..@.....=....l.........Sd-...".<....rstdo.le>..s.t..d.o.l.e.(..h..^ .*\\.G{00020430-....C.....46}#2.0#.0#C:\\Win.dows\\sys@tem32\\.e2..tlb#OLE. Automat.ion.ENor (malENCr.m.aF.. cEC.....m.! OfficgO.f.i.cg..g2DF8D0.4C-5BFA
Data Raw:	01 e2 b1 80 01 00 04 00 00 00 03 00 30 aa 02 02 90 09 00 20 14 06 48 03 00 a8 80 00 00 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 00 08 06 12 09 02 12 80 06 53 f4 64 2d 00 0c 02 22 0a 3c 02 0a 16 02 72 73 74 64 6f 08 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 00 28 0d 00 68 00 11 5e 00 03 2a 5c 00 47 7b 30 30 30

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 20:18:26.726807117 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 20:18:29.727859974 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 20:18:35.765635967 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 20:18:47.772229910 CEST	49172	80	192.168.2.22	45.8.146.139
Aug 11, 2022 20:18:50.789747953 CEST	49172	80	192.168.2.22	45.8.146.139
Aug 11, 2022 20:18:56.796370029 CEST	49172	80	192.168.2.22	45.8.146.139

Statistics

⊘ **No statistics**

System Behavior

Analysis Process: WINWORD.EXE PID: 204, Parent PID: 576

General

Target ID:	0
Start time:	20:18:18
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:	0x13f340000
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	6E172B14	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF7351EEE68A190552.TMP	success or wait	1	6E1F0648	unknown
C:\Users\user\Desktop\~$rdynefile08.11.22.doc	success or wait	1	6E1F0648	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF7351EEE68A190552.TMP	0	366	fd fd 11 71 1a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fd fd 09 00 06 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 01 00 00 00 00 00 00 00 00 10 00 00 02 00 00 00 01 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd	>	success or wait	1	6E1F0648	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	6E0E1925	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	6E0E1925	unknown
C:\Program Files\Microsoft Office\Office14\PROOF\MSSP7EN.dub	unknown	4866	success or wait	1	7FEE916E8B7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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\airdynefile08.11.22.doc	1963480	185	success or wait	2	6E1F0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1A8EAF99.png	0	65536	success or wait	4	6E1F0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5926E0C6.png	0	65536	success or wait	2	6E1F0648	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E1CA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E1CA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E1CA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E1F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E1F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E1F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\7A821	success or wait	1	6E1F0648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\7A821	7A821	binary	04 00 00 00 CC 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 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 A0 CA 53 5A FA AD D8 01 21 A8 07 00 21 A8 07 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E1F0648	unknown

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

Key Value Modified

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\P roducts\00004109F100A0C0010000 0000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1358626844	1426784285	success or wait	1	6E0E1925	unknown

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\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784285	1426784286	success or wait	1	6E0E1925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1358626844	1426784285	success or wait	1	6E0E1925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426784285	1426784286	success or wait	1	6E0E1925	unknown
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	6E0E1925	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	6E0E1925	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	6E0E1925	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	6E0E1925	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	6E0E1925	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	6E0E1925	unknown

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\00004109F1009040010000 0000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784307	1426784308	success or wait	1	6E0E1925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00004109F1009040010000 0000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784308	1426784309	success or wait	1	6E0E1925	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\7A821	7A821	binary	04 00 00 00 CC 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 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 A0 CA 53 5A FA AD D8 01 21 A8 07 00 21 A8 07 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 CC 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 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 A8 07 00 21 A8 07 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E1F0648	unknown

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

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

Disassembly

⊘ **No disassembly**