

JOeSandbox Cloud BASIC



ID: 682622

Sample Name: actionplan doc
08.11.doc

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 19:22:49

Date: 11/08/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report actionplan doc 08.11.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\A7C7EF0B.png	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EBC662B2.png	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{5247F4D0-671C-4B5A-A163-EC9E0BA13D41}.tmp	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{28B9B3A7-C636-414D-ACE1-7B74DE4F80F2}.tmp	11
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{503DE3AF-4050-42E8-8E6B-EBBBB47830BA}.tmp	11
C:\Users\user\AppData\Local\Temp\~DFDA86EB9FE88A2E3F.TMP	11
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\actionplan doc 08.11.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\~\$tionplan doc 08.11.doc	13
Static File Info	13
General	13
File Icon	13
Static OLE Info	13
General	13
OLE File "opt\package\joesandbox/database/analysis/682622/sample/actionplan doc 08.11.doc"	13
Indicators	13
Streams with VBA	14
VBA File Name: ThisDocument.cls, Stream Size: 2879	14
General	14
VBA Code	14
Streams	14
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 357	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




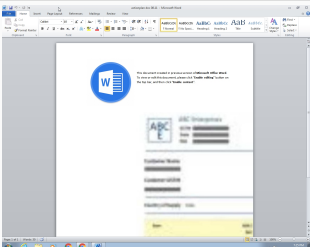
Statistics	15
System Behavior	16
Analysis Process: WINWORD.EXEPID: 2972, Parent PID: 576	16
General	16
File Activities	16
File Created	16
File Deleted	16
File Read	16
Registry Activities	16
Key Created	16
Key Value Created	17
Key Value Modified	18
Disassembly	22

Windows Analysis Report

actionplan doc 08.11.doc

Overview

General Information

Sample Name:	actionplan doc 08.11.doc
Analysis ID:	682622
MD5:	933338ca2c25cf...
SHA1:	e518d12b7bb4ad.
SHA256:	abc8d1097f0249..
Tags:	<div>doc</div> <div>IcedID</div>
Infos:	<div></div> <div></div>

Detection

MALICIOUS

SUSPICIOUS

CLEAN

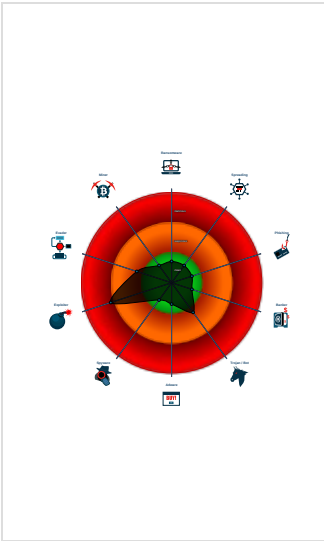
UNKNOWN

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: 2972 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



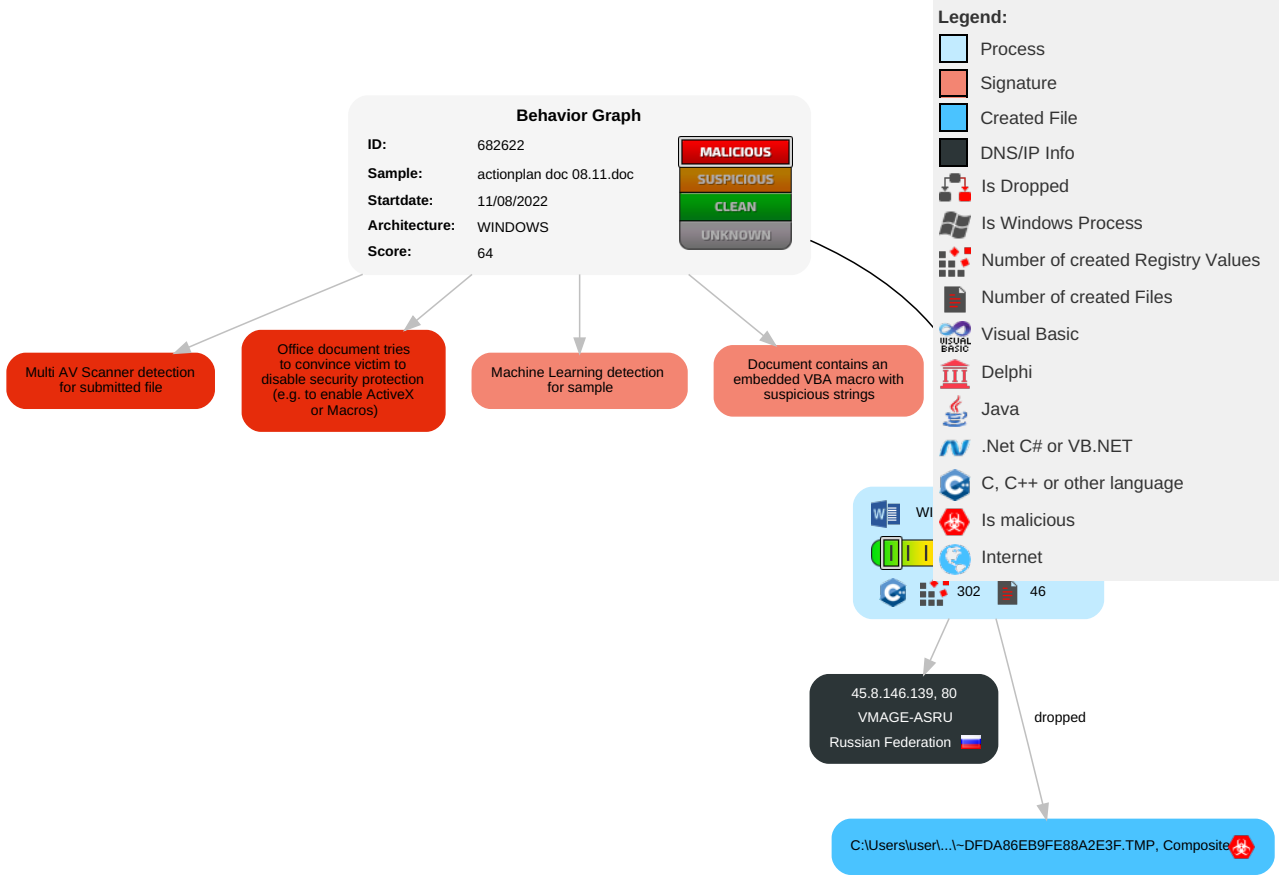
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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

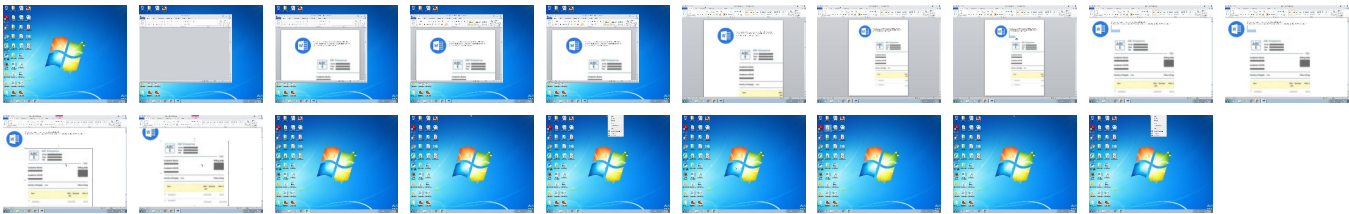
Behavior Graph

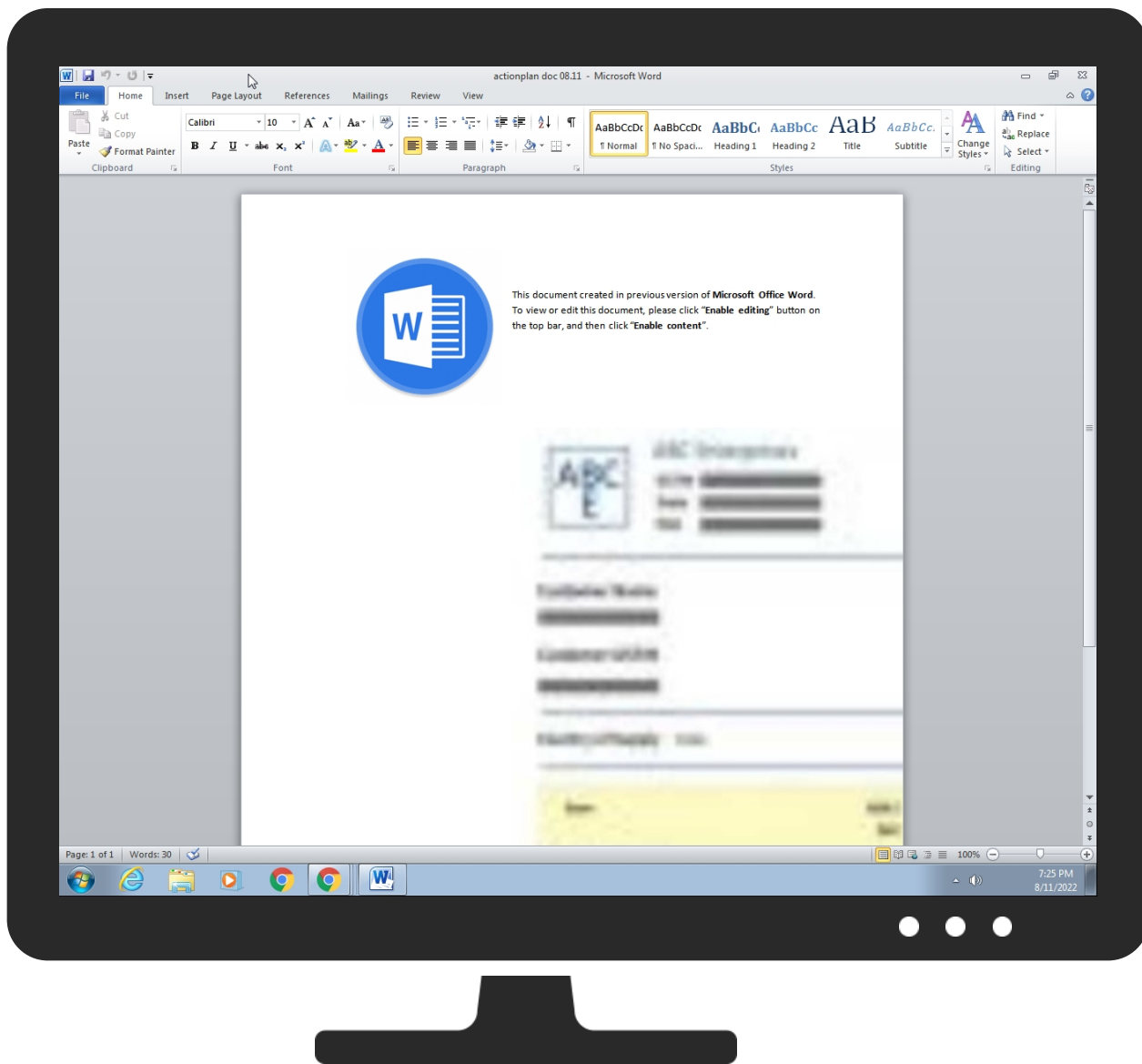


Screenshots

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
actionplan doc 08.11.doc	25%	Virustotal		Browse
actionplan doc 08.11.doc	18%	ReversingLabs	Script-Macro.Trojan.Amp hitryon	
actionplan doc 08.11.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DFDA86EB9FE88A2E3F.TMP	100%	Joe Sandbox ML		

Unpacked PE Files

🚫 No Antivirus matches

Domains

🚫 No Antivirus matches

URLs

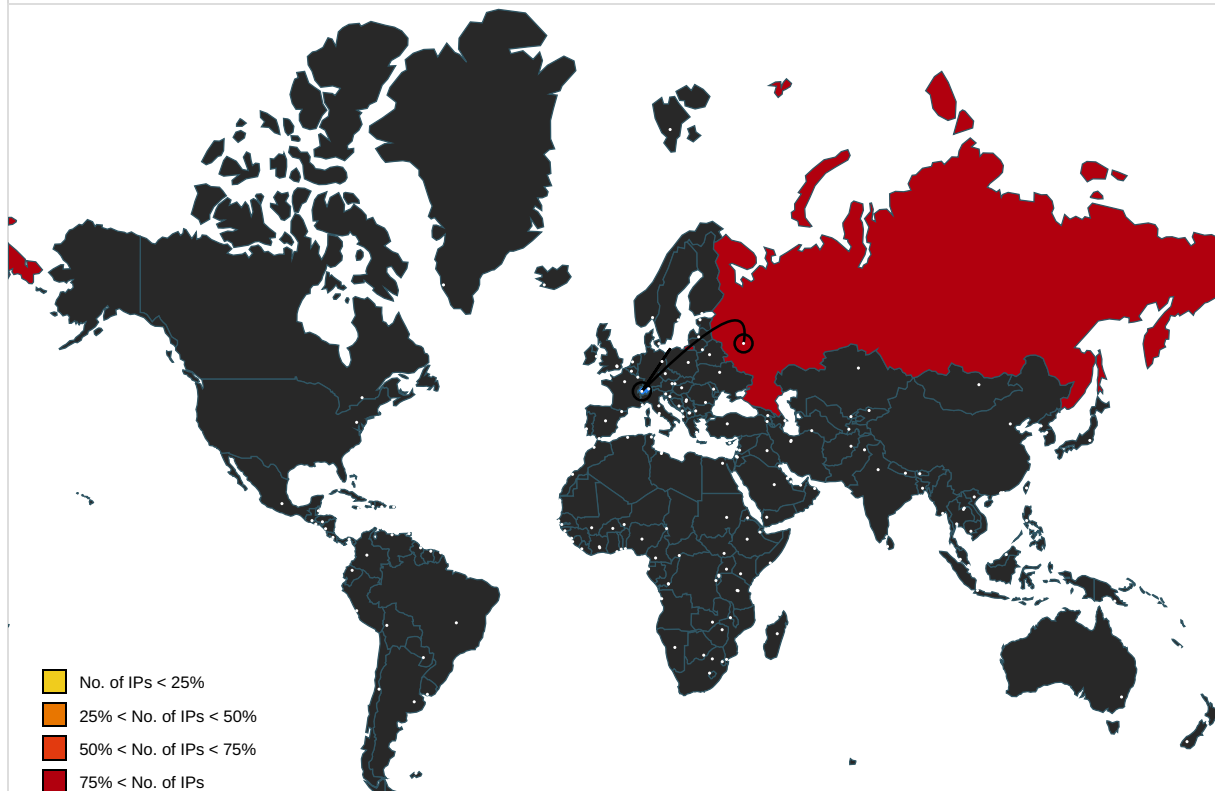
No Antivirus matches

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:	682622
Start date and time:	2022-08-11 19:22:49 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	actionplan doc 08.11.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">• HCA enabled• EGA enabled• HDC enabled• GSI enabled (VBA)• 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:	<ul style="list-style-type: none">• Successful, ratio: 100%• Number of executed functions: 0• Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none">• 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\A7C7EF0B.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:ShliiMUFV26oUc72DI+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.. . +....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...IP...IN..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..!.....A;.....l.,\l@...&....0[.la?..`#2upVW.4.{..c.JMZ..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EBC662B2.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):	256042
Entropy (8bit):	7.978343657002507
Encrypted:	false
SSDEEP:	6144:SD1K9VMjF68qkupr4FNRFrglzGWMOM+IQzPyWae2q:SDEVJBXkR63MWQOHq
MD5:	303B22B7FFAF96496093E5DB3938B563
SHA1:	672080C107AACED7AB0D77E5AA3055ECBFA494DC
SHA-256:	AEF779CE0BA64FA155A6867374198754FCADABCBEB5C378A67A6B6846B18F0BB
SHA-512:	49FD4F26EA3DCE9742D0E5C134C30EB535C58F0B42458AABF546FDD5C053845FC62C65B87AA99478A754A00146BAA0A0088E926CABB7EE2E8FBDD2F6DEBA368
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs..!..!.....IDATx^...fGU.s..8.3...?.3.hh...JTD%....\$)#U ..(\$!..&HB.ol'l.'i...iE..d...r....9}O.5.<...[{.^].....K..j.U.j.Z...~....+<'.=\$.X.....].....q..\$2./...1..u...V^OF.N.W....z& "...d....+*.t....Z.D[.*##A.G.C...3..^C..5.q.....`V.h.c`<Z...23_..U^?.Z....Un.fl.S..1.Y^i .Yo.o.....zH..u.C...I.Y.+...2..... V.U....OZ~...f...n.5...m,zec..'j>=..t'i...+*..+O-O....Z.Z.D~...h....6N..zy.}...W..g..v.j...1: ^un...r0..D.+..k....VdY.@...j.+k..j>..8.=.....^m.VV/<.....rH...[.m....Q.U.t[.....^..8.3]....-.l.h.....r..gl.j..@.W.D..m.\$-.3..AK.[.....Y6.N.>.z....+*=...m.^...cu@...t....t.*.....~....1..+..z.D~.t.D.ky[a..~...+#.].6.....z...O\$...[^%[]].KW....-.r.,!..H..@M.W....W...*....j..h..A[...t..7..e-...k[.my.y.kH.h.h..5.D...6].h.U..3.C[.6.B-}.X!Q.c.v.Z....=D..tm7..L.M.. l./.....V...8..c.....N..[Z{m%t.K....].m..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{5247F4D0-671C-4B5A-A163-EC9E0BA13D41}.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):	5.695659015516093
Encrypted:	false
SSDEEP:	192:XrKiQE9DBeLI+osxibSa8tTC9DBeLI+osxibSa:OtRdBeBfsxiYtedBeBfsxi
MD5:	B14C599CC14F7210575E07FDC866C3EB
SHA1:	5344704C5E6E89E9089756EA18DD67D516FF85C9
SHA-256:	811A1B84CEC06FFB133423471C3FFAF90A52A9A4BAE7ABE1284D402EE4C514F4
SHA-512:	023995D808E60A5AADADBD862D89E6CD1B9AA0A3C85FE7F45AEC230CC568F2B585962DAE3C068ED5B1CC577D12A47E3408130684648C96CCB82D08C858C1B47
Malicious:	false
Reputation:	low
Preview:>.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{28B9B3A7-C636-414D-ACE1-7B74DE4F80F2}.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{503DE3AF-4050-42E8-8E6B-EBBBB47830BA}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.131668560158345
Encrypted:	false
SSDEEP:	12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82lakwkv+4K4o4PlIxHkUZ9/W4c:4LG1ND9Pxn82YkQH7YPHZz
MD5:	782D491C039C3159E569A76FE51EE951
SHA1:	65B2B2026550B9EB2801EEC8126A6020BB86DB7F
SHA-256:	9AA4FE17BC800CE3E07964E969613C6C9450E4DB654C90D887CB4457CCAF7DFE
SHA-512:	EA723E346E90A0AE00F19BF637D96B3297E2E2EB6DD56498B94EEFC1BA698AAF3D15A4B0BE49B63A32A58E82F1E7D2999F2D79F04AE5518411D0C1BC68A548 50
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\~DFDA86EB9FE88A2E3F.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):	60416
Entropy (8bit):	4.160836053762578
Encrypted:	false
SSDEEP:	768:EWZ+IDubA+Mce1WhQvXcLGxVT1kCd1L3Q2wp+TOWLHG9fo+pGFa3y:fQaJ+sWhQvXc2TqCd1jwQOwG/pGFaC
MD5:	485E316369B1B3052319CD5C88638B7C
SHA1:	20FD4D7BA397EECADEDA5112FDBF06C7525CD251
SHA-256:	C75F488BC7F3E621BBD9CD62454381607638B53E227FB4D7CE724FF0CFBFC7568
SHA-512:	FA8A7A74A0E61D06C22589E67AE5F8B4F382720336F8F5F0383844D47595A9273BD183026A3606FC6B64ED99159D9F043560682D0C47910663D9F6F419699CB6
Malicious:	true
Antivirus:	<ul style="list-style-type: none">Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:>.....T.....(.....!...".#...\$...%...&...'.....)..*...+.....-...../...0...1...2...3...4...5...6...7...8...9.....<...=...>...?...?...@...A...K...C...D. ..E...F...G...H...I...J...;...L...M...N...O...P...Q...R...S.....`...V...W...X...Y...Z...].\.....i..._.....b...c...d...e...f...g...h...[...j...k...l...m...n...o...p...q...r...s...^.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\actionplan doc 08.11.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 15:45:53 2022, mtime=Tue Mar 8 15:45:53 2022, atime=Fri Aug 12 01:24:12 2022, length=2255878, window=hide
Category:	dropped
Size (bytes):	1064
Entropy (8bit):	4.571745374864595
Encrypted:	false
SSDEEP:	12:8ykCpgXg/XAICPCHaXRBktB/eLX+W0/xgia6w4ticvbCFPx96w4JDtZ3YilMMEW:8yn/XThOM2/xfaeWfPxP+Dv3qNu7D
MD5:	ACD2F7B50580C02888EF99600751FA8A
SHA1:	581316D47DED63B69D3D16C58A8ED71B8F5FDB50
SHA-256:	C4690451D2ABDE9049C123E466BC7A1413E4711CCED3D9255462D1FBBC6DBBF7
SHA-512:	10003EE7AAD350FC9ACB282515D767A991F38117A0123F0562F06F167316EB4710DC6FC0932B7E337648446B43308C467CEAA42F7995C74E3B8C1727DA12EE9A
Malicious:	false
Reputation:	low
Preview:	L.....F.....3.....3...E3.....I".....P.O.+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.....z.2."..U.. .ACTION~1.DOC.^.....hT..hT.*...r...'.....a.c.t.i.o.n.p.l.a.n. .d.o.c. .0.8...1.1...d.o.c.....-...8...[.....?J.....C:\Users\.#..... .\536720\Users.user\Desktop\actionplan doc 08.11.doc./.....\.....\.....\D.e.s.k.t.o.p.\a.c.t.i.o.n.p.l.a.n. .d.o.c. .0.8...1.1...d.o.c.....,LB)..Ag.....1SP S.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_..

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):	91
Entropy (8bit):	4.656675625186696
Encrypted:	false
SSDEEP:	3:bDuMJlcGHQpxUMCmX1JdQpxUMCv:bCfxjwxjs
MD5:	6102F29798F87437E24FEFC04A0F2955
SHA1:	BE0A2C563433AFA7781D477223A3029C1A6BA45D
SHA-256:	0A12578297ADAD563C7B4F4FC4FF79650D61FE1F105F2FC2B4449BAF1CD24C57
SHA-512:	480E8BB320CE6EF2A1AE34B82259821B0C533ECB7DE199394283DE305161600553482ABE35894FDA95DB6484B8E86429BD85D43EF1DFBD5D14D96700FE28C77F
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..actionplan doc 08.11.LNK=0..[doc]..actionplan doc 08.11.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:vrJlaCkWtVyaJybdJyIp2bG/WWNJbilFGUld/l:n:vdsCkWtz8Oz2q/rViXdH/I
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDF533BC9E428B0637562AF A
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\Desktop\-\$tionplan doc 08.11.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:vrJlaCkWtVyaJybdJyIp2bG/WWNJbilFGUld/n.vdsCkWtz8Oz2q/rViXdH/I
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AFA
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

Static File Info	
General	
File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.99386898063047
TrID:	<ul style="list-style-type: none">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:	actionplan doc 08.11.doc
File size:	2349822
MD5:	933338ca2c25cfda5c124455216d6709
SHA1:	e518d12b7bb4addf1dc041a05575031890c1b4d7
SHA256:	abc8d1097f0249c749f2c7d7058be1b39c88e21d26d45d76985c989289565214
SHA512:	57d89f7b2319e6725bc72e06b3e00b13b4e23445a723bb84fc3d0d199b8546b7e30de68c4b90a3244aad7b974c3e6bbe8695ab0cacac8aef18ccceae3c741c5
SSDEEP:	49152:4ek4NG5JJHblCOlciYIHmWvTXaZ4D18AnhBmqB8Rplib7IFysec7htl:rkV5JJlLlcYIHTvTX/15v9bZFyseghi
TLSH:	ACB5337CC120B149C3363F5C594A05B98C9F5E67F7C498395E2F680AE56EA2A4ED0ACC
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/682622/sample/actionplan doc 08.11.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: 2879	
General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2879
Data ASCII:	...Attribute VB_Name = "ThisDocument"...Bas...1Normal...VGlobal!.SpaceIfFalse.JCreateTable.PreDeclareId..#True."Expose.TemplateDeriv.\$CustomLizC.P....D.?PtrSafeFunction...Lib"user.32"Alias"KillTimer"(ByVal.....!AsLong/,...-....).
Data Raw:	01 1f b4 00 41 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: 357	
General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	357
Entropy:	5.2699223718129895
Base64 Encoded:	True
Data ASCII:	ID="{8C36501C-849B-4489-8357-D40B997E00E4}"..Document=ThisDocument/&H00000000..Name="Project"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="C0C2717775777577757775".DPB="8082313232323232"..GC="4042F1F2F2F2F20D"....[Host Extender Info]..H000000
Data Raw:	49 44 3d 22 7b 38 43 33 36 35 30 31 43 2d 38 34 39 42 2d 34 34 38 39 2d 38 33 35 37 2d 44 34 30 42 39 39 37 45 30 30 45 34 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

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

System Behavior

Analysis Process: WINWORD.EXE PID: 2972, Parent PID: 576

General

Target ID:	0
Start time:	19:24:13
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:	0x13f3a0000
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	6E002B14	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DFDA86EB9FE88A2E3F.TMP	success or wait	1	6E080648	unknown
C:\Users\user\Desktop\~\$tionplan doc 08.11.doc	success or wait	1	6E080648	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:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	6DF71925	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	6DF71925	unknown
C:\Users\user\Desktop\actionplan doc 08.11.doc	1872006	184	success or wait	2	6E080648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EBC662B2.png	0	65536	success or wait	4	6E080648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSOA7C7EF0B.png	0	65536	success or wait	2	6E080648	unknown


Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E05A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E05A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E05A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E080648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E080648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E080648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\78CC5	success or wait	1	6E080648	unknown

Page 17 of 22

Disassembly

 No disassembly