

JoeSandbox Cloud BASIC



**ID:** 682661

**Sample Name:** cis-broadband  
invoice 08.11.22.doc

**Cookbook:**

defaultwindowsofficecookbook.jbs

**Time:** 20:23:23

**Date:** 11/08/2022

**Version:** 35.0.0 Citrine

# Table of Contents

Table of Contents	2
Windows Analysis Report cis-broadband invoice 08.11.22.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\ID6296BE7.png	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EAA784BC.png	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{8F2FE185-290C-42B7-B879-93E4A4E5C87A}.tmp	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{05B44CFC-9A30-42B4-97EB-72C438F00945}.tmp	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{37EDF262-52CE-44C0-9FEE-A4113696C4D3}.tmp	11
C:\Users\user\AppData\Local\Temp\~DFD78FF001C09C6661.TMP	11
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\cis-broadband invoice 08.11.22.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\UProof\ExcludeDictionaryEN0409.lex	12
C:\Users\user\Desktop\~\$s-broadband invoice 08.11.22.doc	13
Static File Info	13
General	13
File Icon	13
Static OLE Info	13
General	13
OLE File "opt\package\joesandbox/database/analysis/682661/sample/cis-broadband invoice 08.11.22.doc"	13
Indicators	13
Streams with VBA	14
VBA File Name: ThisDocument.cls, Stream Size: 2837	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	14
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: 2952, 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

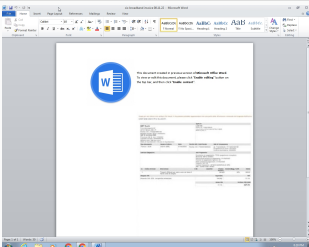
# Windows Analysis Report

cis-broadband invoice 08.11.22.doc

## Overview

### General Information

Sample Name:	cis-broadband invoice 08.11.22.doc
Analysis ID:	682661
MD5:	91ca71d98c0e42..
SHA1:	b8b01ee5940864.
SHA256:	373856a75b7840.
Tags:	<div>doc</div> <div>icedID</div>
Infos:	<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...

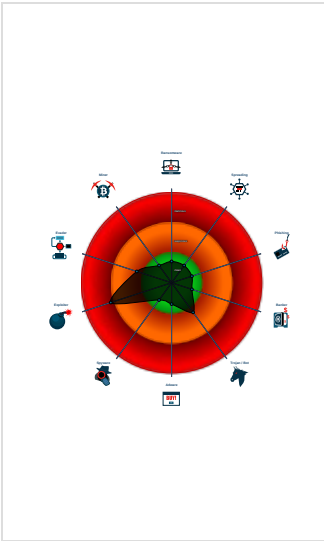
Document contains an embedded V...

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: 2952 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



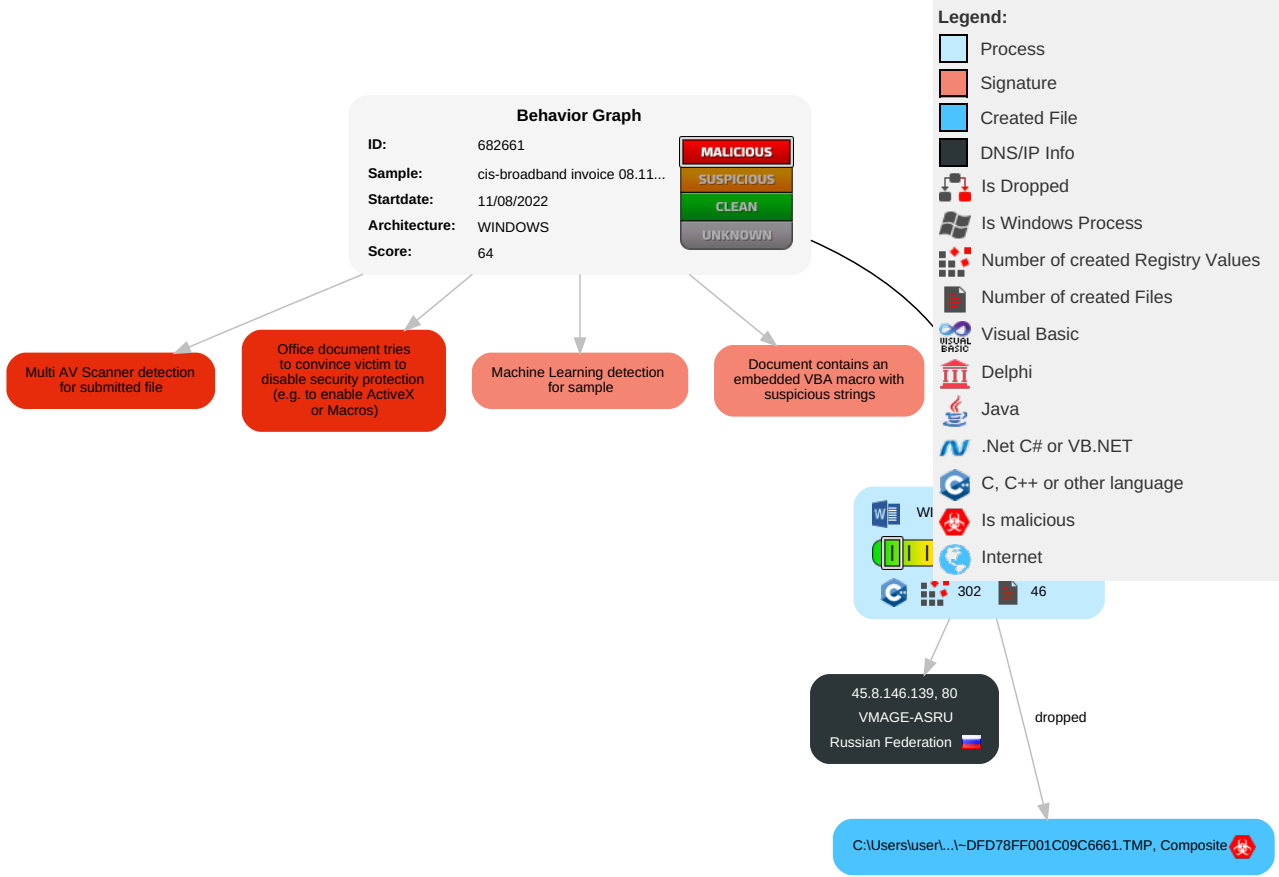
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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

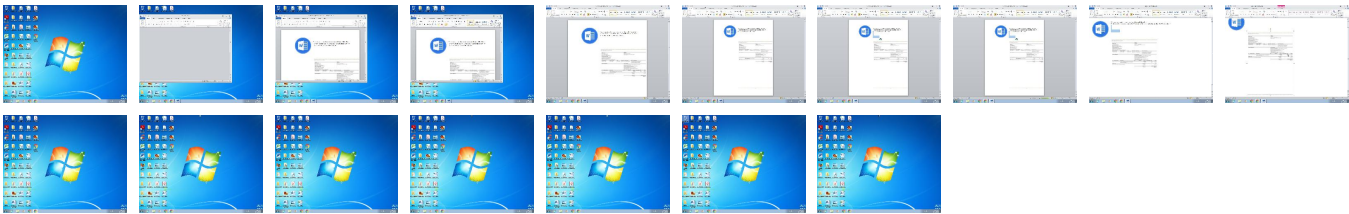
## Behavior Graph

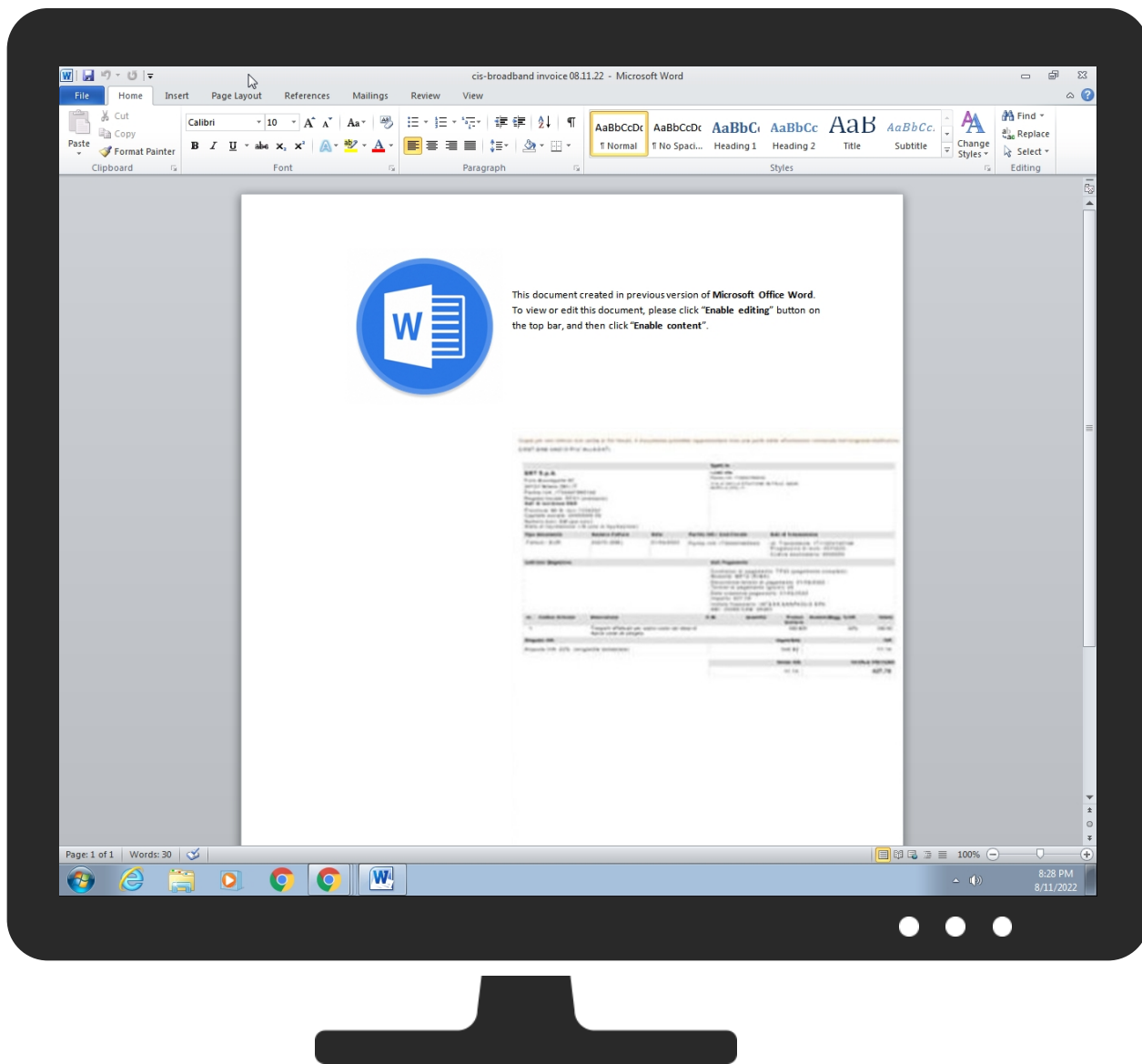


## Screenshots

### 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
cis-broadband invoice 08.11.22.doc	25%	Virustotal		<a href="#">Browse</a>
cis-broadband invoice 08.11.22.doc	15%	ReversingLabs	Script-Macro.Trojan.Amp hitryon	
cis-broadband invoice 08.11.22.doc	100%	Joe Sandbox ML		

### Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DFD78FF001C09C6661.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:	682661
Start date and time:	2022-08-11 20:23:23 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cis-broadband invoice 08.11.22.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:	<ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
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"><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



<b>C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D6296BE7.png</b>	
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):	256229
Entropy (8bit):	7.979121196288089
Encrypted:	false
SSDEEP:	6144:xcZ1/hftNLDurggURJVg/41g/U14PThyg2vnHkX005Pk:xcZ15ftNLy5MJMM4Ff2vHI00y
MD5:	9D69322290350F00911BF601D1EB0548
SHA1:	2CC5B16D959BCCF6457C881EC3106EDD846E77E6
SHA-256:	4B4AA777CC69D3E05C61AA4F57475E1F41B4AA8DA0463AD4EBF2CA98AD5A927
SHA-512:	C7CC06CDCCD2E9DA32FBD0C0BD4B5F5CFBC937C980CBB66DDFD2953DFC7DD4EB9D69E19EA72BF3D291D4F229CAE015A9C83040AA5DE23563B1D28BDF0E9875CCD
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs.....!.....IDATx^.....fEu.....&.....c....Fc....b41q`FIAQ....44 8+m....CL'!...!*Q...>.g.!H...?g.uzuQ=....TW.Z.V..j].....?. V1...P.JO.K.h..IO.*7.oi...=:i.l.'oV.V7.K@...6.%j.".....l.....[ .5Td= y!.....P.....d>Q..ke....l9.H^..\\....h.cm....'1.....+\$.....S.....J...g....U.8.....3.h.ni5...:Z^'.j...&.-3.....8Q...j..[Y...t.^..zh..#..._E-W.5...!Q..U..V...*.Z..j.[.....m.=z;2.5...8./..K.u...U~Li-oV.t..A.!{;.k.1z...+....[> _S..\..l.W.D...Nz.^..`r.....b..z.^>..{.Te..2N...~.....T=..4...he&....X.m..V.....D..5]...j...%L.....F=YW.3..Z..*.h.S..e..)jz9...IK~O.E.L.@...Z~E.z.D..l...B..#\$.j...u.^.....t.c.d..{2.#.h.W...U _=PudH.*....'2?FK:q[~....aL.Mg..J..+!/*Z='N.h..D..t..G..m..@hL..3..Zz.3.b.....ze.LO>..q.5.5.=...m..['^..8....c.6.5..gh1F_n.U^..n.%G.....N.*....eA~.X:..j..Y..6.^....[[.e@'!~.%g.Z...t...L..R&5..j.Q.IE...ul.....D.W~..

<b>C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EAA784BC.png</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 410 x 568, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	61935
Entropy (8bit):	7.988218918927523
Encrypted:	false
SSDEEP:	1536:vFo53cC4vJ7Y8qgUmqhlIPi2MM+ikJU78DPaFx:vy53qv6nmll0l2ngJAEan
MD5:	4800E90C87A78932178C7D338BA32F43
SHA1:	8006244EDAFF9A31546A17FCF99CB61DA4F69417
SHA-256:	8CD11EB654C64C7315F7B2904D123532F7993FAF2F210B250C4C4D670200FF73
SHA-512:	58994BDC81FF937B05B307C161F852383DAA8504EA17522CD96CDE6EBF99E4992BA64DBEA532424AC16FBD8273999295DBBB74E48A77AAB2122C5701633DC773
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....8.....X.L...IDATx..ji..F~..r.E.l.u..3....L...^TR.....DF...*l.e.j.:U.L&...pq.p.1.HD.Z.@..6..._cc.....>.n....2v..c.%...).G.? ...>k...bf.....c0.sy...\$.a...<.....>"=X1.....1.^ ].....! .....!E..c.#.T.....'.....\$6&L1.0.H...X&"..cp.l...p.>..?.@?.1.Tp....Y...=D.j]....w.=~..yp...{x/.....d}1.G.h..b."1..-}0x...O.....<.&n..0.1...el.....""...C<t..A.H..4O.L.G...v...6Bd...W[>..;W...E.#<..s.^...Q...B.o.=l.IB[...1.ab.\$D.:WB\$O..V..>..k...y~.w"...A...-D...;l.4b.D..E".3...1..f....J~xv.35G&&...?acR...P.N....)U.JJ....F.l...c\$... ..a..z&...1..l...D...b.A4.....U..._D.Z...E.6.G9t.=.qj...^L.\$;...>..S&dD.X... 1...0.{~w..P....1.U(....j.PM.....9J..[O2...).12swy%3..M?NGt_.....Z.....?F..+.....[4@.=.....;..6..i.c..qH4...Ll..8.kl...=""!..h.g7.\'.....Bb.A..f..o).+..`..++..?u..<i.M..Gvs..@w.\$2X..'[.h.8h.3..G.g.E...3..d)..V^./\$)...."%...F...~...s.1@ ....dE.8D ..d.....N.z.(...

<b>C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{8F2FE185-290C-42B7-B879-93E4A4E5C87A}.tmp</b>	
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):	4.045024044508011
Encrypted:	false
SSDEEP:	384:DtmYVXXo+cY/+eoNaN9gCXtOYVXXo+cY/+eoNaN9gC:U2XXoWJoNAPI2XXoWJoNAP
MD5:	EEC2F5D84BC16802A1BD4F4657EEA2A0
SHA1:	92CFA9B62BCA6A2B379BE2885C3203C32FFD4AA1
SHA-256:	144729E8D4886799AA9CCE94DFE5385783F40A312BE2B619595EE7A03CF58C2F
SHA-512:	1AE959E1EC7A1A2D13E59CAD9855DEB33EE5CC0CBBD867A7591E219F638B0866BBC384FE5650FC2DA422EC9E24EBC0661143F2927BE519AB7394C3DF5779FD27
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{05B44CFC-9A30-42B4-97EB-72C438F00945}.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{37EDF262-52CE-44C0-9FEE-A4113696C4D3}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.1256146146486787
Encrypted:	false
SSDEEP:	12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82lrBkwkvGtb4rO4EO4PII/OHkUZ6/W4c:4LG1ND9Pxn82Tklb0OVOYhOHRz
MD5:	D25E22EDE76A3AE649DCCCB2F91BE4F7
SHA1:	BE40CC62EFCBE175C501681C0B912AC4587E2927
SHA-256:	22325040E5A65E483EA6AD15DE02293CBD0E3B5DCBC99302C6E1D223B7E79CEE
SHA-512:	A2EED97A7DA0823A276CAA4434D5002A2A0D044F7A45CFF3AFD429B5CF8D751D00978A99D48AB31847DF16FBAA59D42FE01895B81DE44F7362E0240BC01A6C 0F
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\~DFD78FF001C09C6661.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):	4.158295628290084
Encrypted:	false
SSDEEP:	768:+A+wLdVcQDH5tQ+un5aplP3c2XoW+B5WFG05GyA6WGLap:xJEYHs+un5aplP3i5KG7j7GLap
MD5:	07465F5EEE019870312FF551E07C3313
SHA1:	DC7609DD24CAFB2B0325D03A7ED80AB85E839243
SHA-256:	BE15A6906B90D23EF4411049F7E4B70AFFABBF069A2B9C07A6863ED6057089C0
SHA-512:	BA0A5313E7967B710AE1CCF704BF334FFE1A4941DDDF31030158562EE7B6EA80BD9A858AAF8705BD0CD7158EE476A1CACB55837426457FB6BA02A80C7FCD53 F7
Malicious:	true
Antivirus:	<ul style="list-style-type: none"><li>Antivirus: Joe Sandbox ML, Detection: 100%</li></ul>
Preview:	.....>..... .....T.....( .....l...".#.\$...%...&...'.....).....*...+.....-...../...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...].\.....i..._.....b...c...d...e...f...g...h...[...j...k...t...m...n...o...p...q...r...s...^.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\cis-broadband invoice 08.11.22.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 02:27:16 2022, length=2298962, window=hide
Category:	dropped
Size (bytes):	1114
Entropy (8bit):	4.569901986366081
Encrypted:	false
SSDEEP:	12:8jjWQEu0gXg/XAICPCHaXNBQIB/SxXX+W19Y5iL9zwicvb8XNq9zwDtZ3YiIMMER:8HF4/XT9SU39ZLBTewXkBwDv3qTau7D
MD5:	A349CC0897655850144A4430DFE8E24C
SHA1:	E7258974F336299DA09942F9CCFB12A56056D143
SHA-256:	5B0F596E730C773AE8E9B591EB27F018DD95030331A203B9721DB20B646FB21F
SHA-512:	FCEDF2A31D1BEDE67643B2CDB30F3F99A638094AD8DD530203B70AD923B51EC9C5878233DEA146E2EF07D3EFC5DAEB61D1C28F13318734533613B5BEC4FF4FA
Malicious:	false
Preview:	L.....F....~.....3.....3.....k....R.#.....P.O. ....+00.../C:\.....t1....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.....2.R.#..Ui. .CIS-BR~1.DOC..f.....hT..hT..*...f.....*.....c.i.s.-.b.r.o.a.d.b.a.n.d. .i.n.v.o.i.c.e. .0.8...1.1...2.2...d.o.c.....-...8...{.....?J.....C:\Users\..#.....\\116938\Users.user\Desktop\cis-broadband invoice 08.11.22.doc.9.....\.....\.....\.....\.....D.e.s.k.t.o.p.\c.i.s.-.b.r.o.a.d.b.a.n.d. .i.n.v.o.i.c.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.

<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):	111
Entropy (8bit):	4.815919561621978
Encrypted:	false
SSDEEP:	3:bDuMJleUHELgLplbUmX1bWEHELgLplbUv:bCU7Dbuu7Db2
MD5:	A649133664619D3CDC98418B3EC97D2A
SHA1:	0F597DDC41928FBB93544E5972B07D14365B386F
SHA-256:	3C7978588FF30B4B1BA90073AC13363A73058CAFB8F79B4189CC541283D07D75
SHA-512:	C819B43C5B49FF8D672525C903F2765ED7974D6CF017A6E5860C390D50A01946AF62A123FD5E1E98672A96901DC55E9DCFCAE2F880780653C27EAFB736201A6
Malicious:	false
Preview:	[folders]..Templates.LNK=0..cis-broadband invoice 08.11.22.LNK=0..[doc]..cis-broadband invoice 08.11.22.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:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB

SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDf1C54CA0D4
Malicious:	false
Preview:	..

<b>C:\Users\user\Desktop\~\$s-broadband invoice 08.11.22.doc</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:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265:5
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

<b>Static File Info</b>	
<b>General</b>	
File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993383170496904
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:	cis-broadband invoice 08.11.22.doc
File size:	2298962
MD5:	91ca71d98c0e42e0446e9157fc83e1f2
SHA1:	b8b01ee5940864817c670187dfc1cb9a663c79a8
SHA256:	373856a75b78406d26cfbb41cbbba7041bad1e56a3304ba17376b294bc773eee
SHA512:	f5ca7cb3645558bd8e390d34721ce9abfd93912c56a9470e7f2e5ebab52bcd82c5740e90e3d0f8d0710fdc313cd9570e3fee05f897d1883af04df2773740717
SSDEEP:	49152:l5cNRR+7lr64bJwEeTVzVSqJl4VBnLiiYRCcuaNTSIY:l5cbR+7bmEcVQ4VBnOiYGCTG
TLSH:	FAB53374A4EC9D32EA4FA3B1D78634E5F6C97C8D30B84657671F1902D0AAA1E03E21F5
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.....hl.3..H.Q.*.;.=.y... n.....yo.....[vrf..A..6..3[>_...-K....\NH!....<..r...E.B..P...<_.

<b>File Icon</b>	
	
Icon Hash:	e4eea2aaa4b4b4a4

<b>Static OLE Info</b>	
<b>General</b>	
Document Type:	OpenXML
Number of OLE Files:	1

<b>OLE File "/opt/package/joesandbox/database/analysis/682661/sample/cis-broadband invoice 08.11.22.doc"</b>	
<b>Indicators</b>	
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: 2837**

**General**

Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2837
Data ASCII:	.h.Attribute VB_Name = "ThisDocument"...Bas..1Normal...VGlobal!.Spac.IfAlse.JCrea.tabl. .Pre decla..Id..#Tru."Expose..TemplateDeriv.\$CustomlizC.P....D.? PtrSa.fe Function .... L ib ".user32" .Alias "SetTimer" (ByVal.... As Long.1, ..*.....
Data Raw:	01 68 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:	5.3000173575513605
Base64 Encoded:	True
Data ASCII:	ID="{4ACDA209-D3D8-436D-A5D9-6DA204CC3EA8}"..Document=ThisDocument/&H00000000..Na me="Project"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="EBE9F817E71BE7 1BE71BE71B"..DPB="D6D4C50C5B1C471D471D47"..GC="C1C3D2D7D3D7D328"....[Host Extend er Info]..
Data Raw:	49 44 3d 22 7b 34 41 43 44 41 32 30 39 2d 44 33 44 38 2d 34 33 36 44 2d 41 35 44 39 2d 36 44 41 32 30 34 43 43 33 45 41 38 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 00 00 00 00

**Stream Path: VBA/\_SRP\_2, File Type: data, Stream Size: 5108**



# System Behavior

Analysis Process: WINWORD.EXE    PID: 2952, Parent PID: 576

## General

Target ID:	0
Start time:	20:27:17
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:	0x13f030000
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	6DF32B14	CreateDirectoryA

### File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\--DFD78FF001C09C6661.TMP	success or wait	1	6DFB0648	unknown
C:\Users\user\Desktop\--\$s-broadband invoice 08.11.22.doc	success or wait	1	6DFB0648	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	6DEA1925	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	6DEA1925	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\pcis-broadband invoice 08.11.22.doc	1964332	185	success or wait	2	6DFB0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSOD6296BE7.png	0	65536	success or wait	4	6DFB0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EEA784BC.png	0	61935	success or wait	1	6DFB0648	unknown

## Registry Activities

### Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6DF8A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6DF8A5E3	RegCreateKeyExA



Key Path	Completion	Count	Source Address	Symbol
----------	------------	-------	----------------	--------

HKEY_CURRENT_USER\Software\Microsoft\VBAL7.0\Common	success or wait	1	6DF8A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6DFB0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6DFB0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6DFB0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\7A1DB	success or wait	1	6DFB0648	unknown

### Key Value Created

[illegible]



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	6DEA1925	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	6DEA1925	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	6DEA1925	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	6DEA1925	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	6DEA1925	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	6DEA1925	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	6DEA1925	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	6DEA1925	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\7A1DB	7A1DB	binary	04 00 00 00 88 0B 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 88 0B 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	success or wait	1	6DFB0648	unknown






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

FF

Disassembly

 No disassembly