

JoeSandbox Cloud BASIC



ID: 682661

Sample Name: cis-broadband
invoice 08.11.22.doc

Cookbook:
defaultwindowsofficecookbook.jbs

Time: 20:07:12

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\83C87933.png	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FAAE737A.png	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{10C83EEE-519A-4BAE-9701-FB36EC529A4B}.tmp	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A4DFC439-0F12-4756-9A4F-0DC4BA4A60ED}.tmp	11
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{CDB32EEE-51F1-404D-8EA2-3142A158663B}.tmp	11
C:\Users\user\AppData\Local\Temp\~DF1CF4A488C21180D9.TMP	11
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\cis-broadband invoice 08.11.22.LNK	12
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	14
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	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




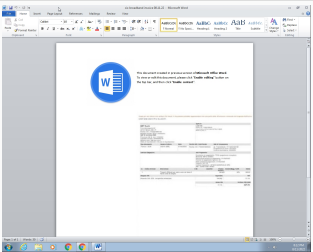
Statistics	15
System Behavior	16
Analysis Process: WINWORD.EXEPID: 2032, Parent PID: 576	16
General	16
File Activities	16
File Created	16
File Deleted	16
File Read	16
Registry Activities	16
Key Created	16
Key Value Created	17
Key Value Modified	18
Disassembly	22

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>lcedID</div>
Infos:	<div></div> <div></div>

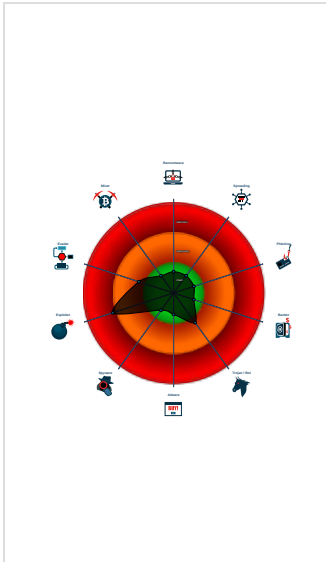
Detection

<div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div>	
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: 2032 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



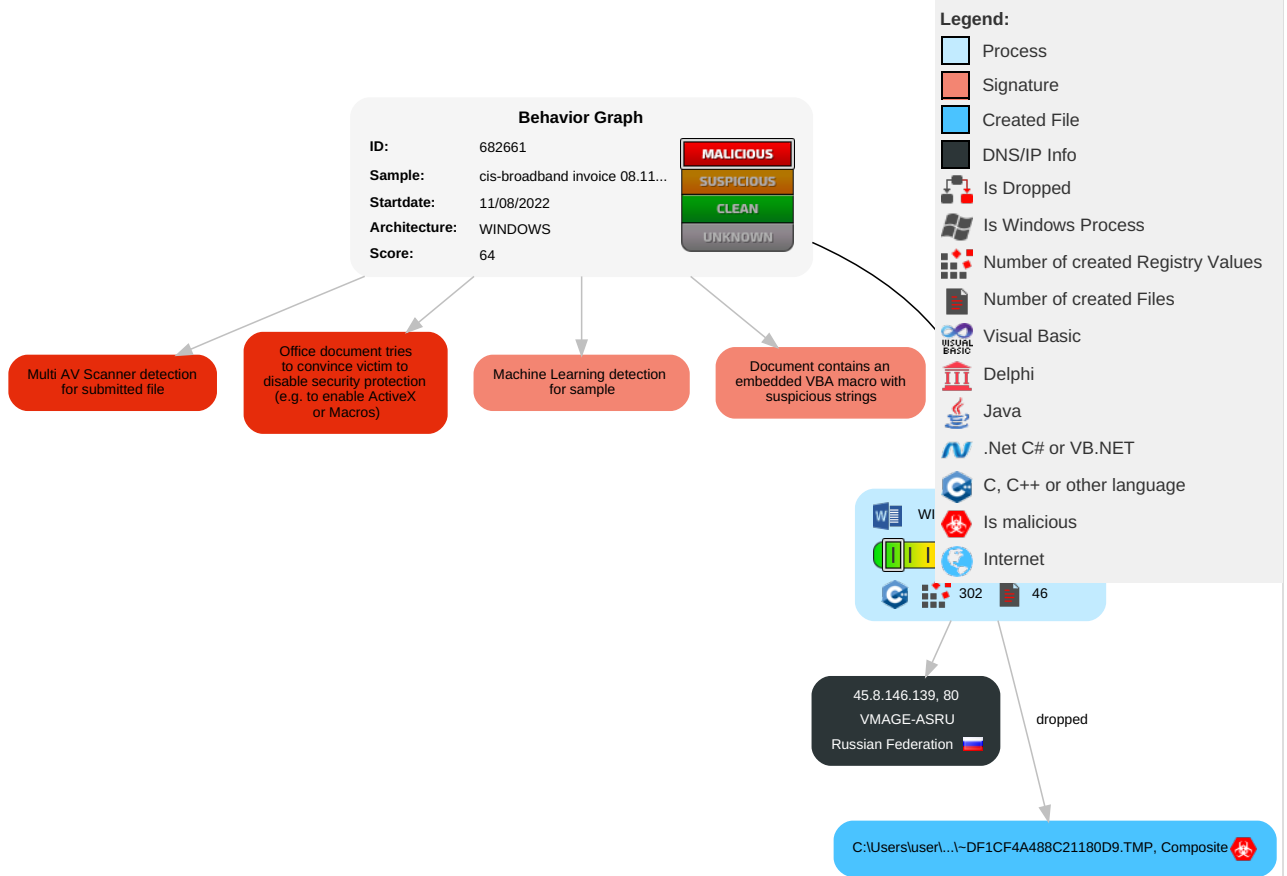
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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

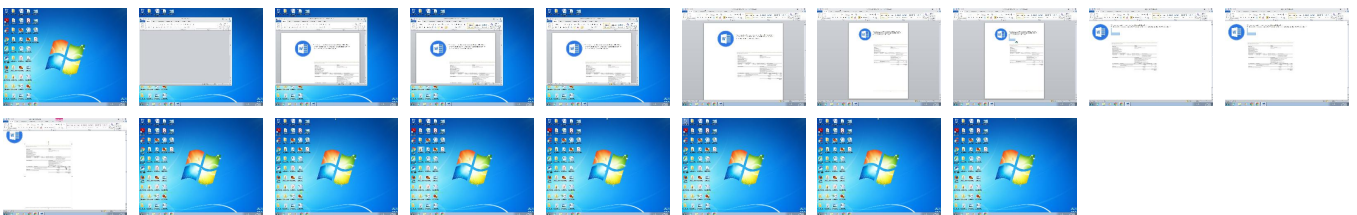
Behavior Graph

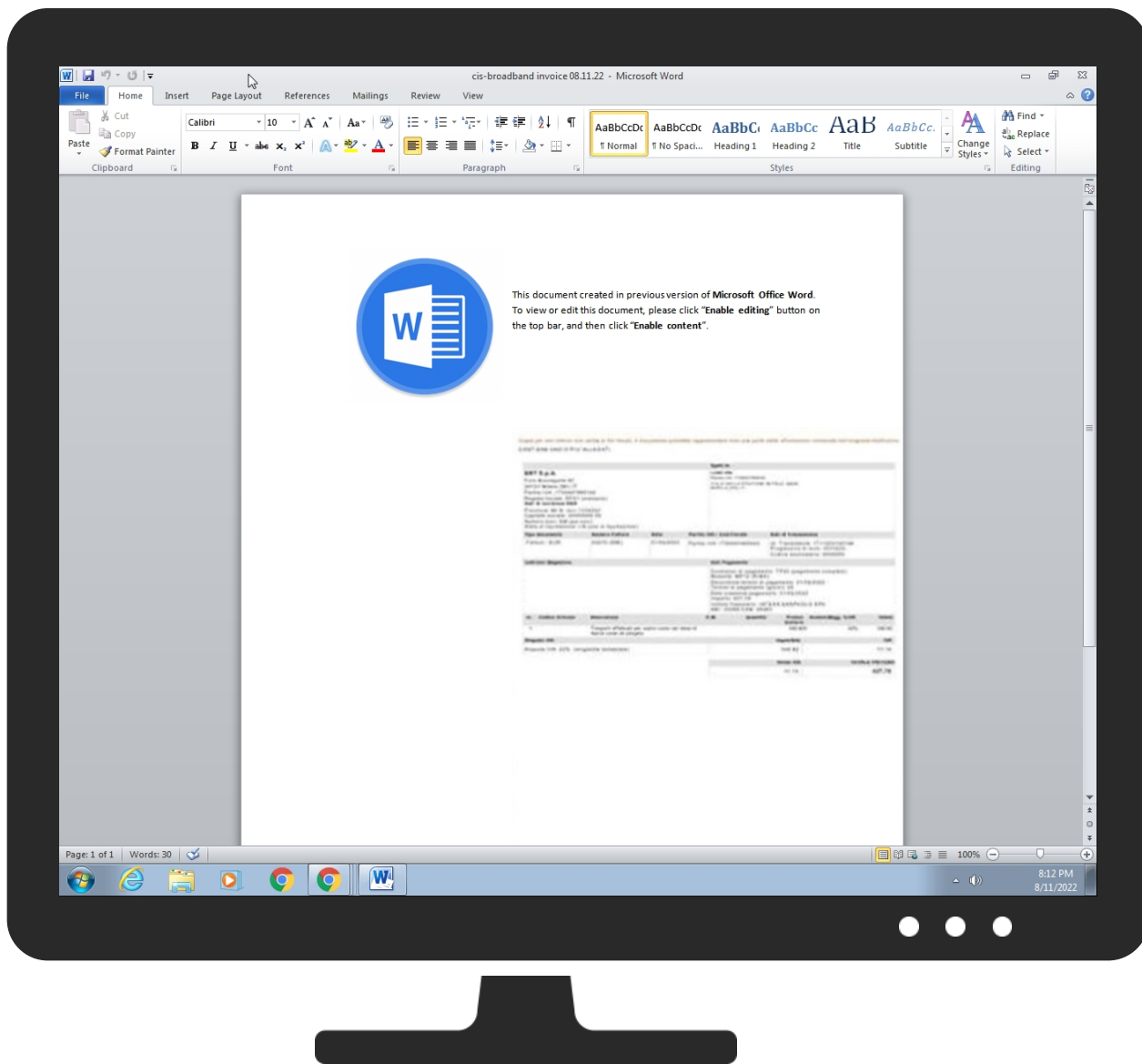


Screenshots

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		Browse
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\~DF1CF4A488C21180D9.TMP	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

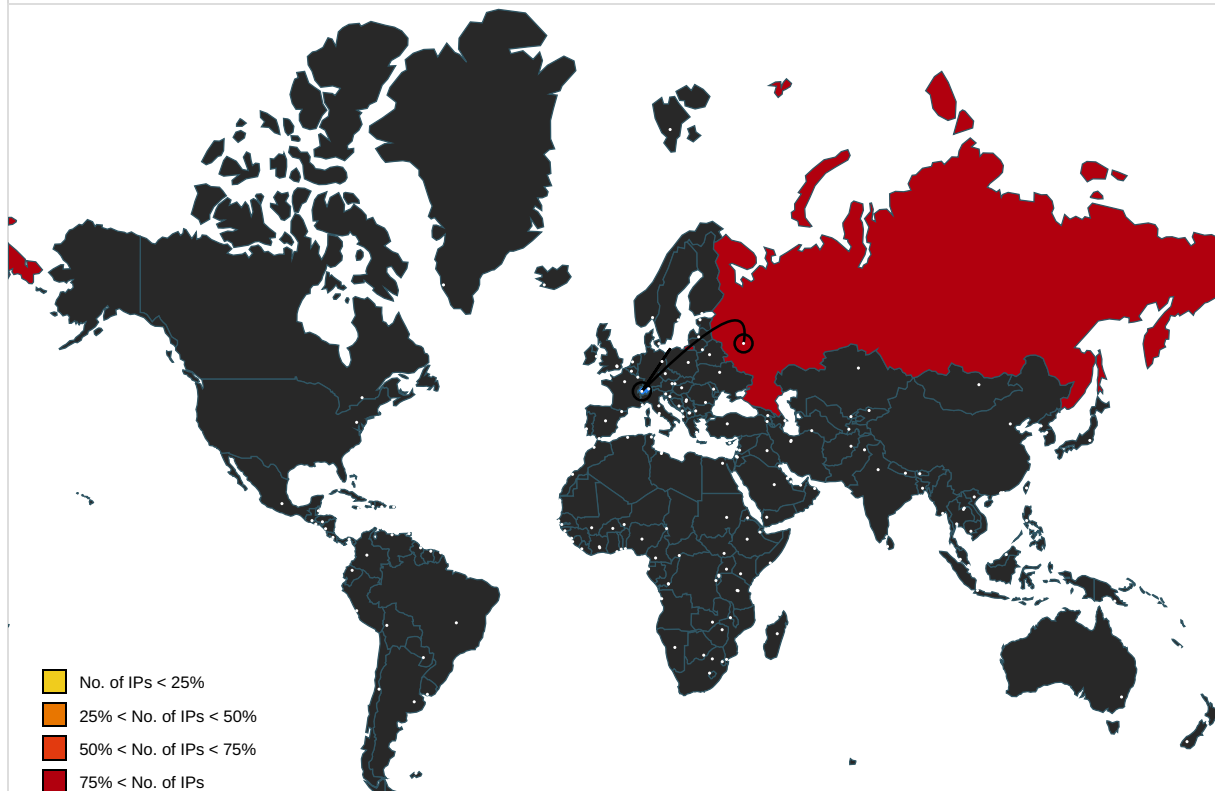
⊘ No Antivirus matches

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 20:07:12 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 29s
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)
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\83C87933.png

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:vFo53cC4vJ7Y8qqUmqhllPI2MM+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.-.lr.E.l.u..3....L...^TR-----DF...*l.e.i.:U.L&...pq.p.1.HD.Z.@.6..._cc.....>.n...2v..c.%...).G.? ...>k...bf.....c0.sy..\$...a...<.....>".=X1.....1.^ l.....l'E..c.#.T.....'.....\$6&L1.0.H...X&".cp.l...p.>..?.@?.1.Tp.....Y...=D.]...).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.B{...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.J....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.(...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FAAE737A.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):	256229
Entropy (8bit):	7.979121196288089
Encrypted:	false
SSDEEP:	6144:xcZ1/hftNLDurggURJVg/41g/U14PThyg2vnHkX005Pk:xcZ15ftNLy5MJMM4Ff2vHI00y
MD5:	9D69322290350F00911BF601D1EB0548
SHA1:	2CC5B16D959BCCF6457C881EC3106EDD846E77E6
SHA-256:	4B4AA777CC69D3E05C61AA4F57475E1F41B4AA8DA0463AD4EBF2CA98AD5A927
SHA-512:	C7CC06DCDD2E9DA32FBDC0BD4B5F5CFBC937C980CBB66DDFD2953DFC7DD4EB9D69E19EA72BF3D291D4F229CAE015A9C83040AA5DE23563B1D28BDF0E98175CCD
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= yl.....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...r!Q..U..V...*.Z..l.[.....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..#\$.]...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:..}.Y..6.^....[[e@'!'-.%g.Z..t...L..R&5..j.Q.IE...ul.....D.W~..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{10C83EEE-519A-4BAE-9701-FB36EC529A4B}.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):	5.689391970203913
Encrypted:	false
SSDEEP:	192:e8nbKt+LNUoNtsNqkgCWa/+trLNUoNtsNqkgCWa/+utgeoNaN9gCatPeoNaN9gC
MD5:	1DE4CCBB960FD51F83DB2C92A88CED6E
SHA1:	CF09D3848F11A734379DA3287D4141B4587FD825
SHA-256:	4261BD30C647405055B764869DD518447F4BF1D0A46D98F05399D91C3EFD1E1F
SHA-512:	305970CD8D435B19261BEB557B6D6286DB156B5A194E6B62A8C772D92FA8758A0BA7143BF239A06ABC1BB4D1B242E2B5026ABA38654BE7127E582D4F1B3C2AF9
Malicious:	false
Reputation:	low
Preview:>.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A4DFC439-0F12-4756-9A4F-ODC4BA4A60ED}.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:4LG1ND9Pxn82Tklb0VOYhOHRz
MD5:	D25E22EDE76A3AE649DCCCB2F91BE4F7
SHA1:	BE40CC62EFCBE175C501681C0B912AC4587E2927
SHA-256:	22325040E5A65E483EA6AD15DE02293CBD0E3B5DCBC99302C6E1D223B7E79CEE
SHA-512:	A2EED97A7DA0823A276CAA4434D5002A2A0D044F7A45CFF3AFD429B5CF8D751D00978A99D48AB31847DF16FBAA59D42FE01895B81DE44F7362E0240BC01A6C0F
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{CDB32EEE-51F1-404D-8EA2-3142A158663B}.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:	4826COD860AF884D3343CA6460B0006A7A2CE7DBCCCD4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:

C:\Users\user\AppData\Local\Temp\~DF1CF4A488C21180D9.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):	4.155089614218598
Encrypted:	false
SSDEEP:	768:nA+wbd26bDH5ym+uS5aT02rw2XoWdBNW4GIgByA6NGLaG:A9zvHt+uS5aT02r3N7GFjEGLaG
MD5:	F238058197930192DDB69D359BE7775E
SHA1:	C0D3C058633556E8F4521139B63119DFF0C7E4E4
SHA-256:	DC906CE77C80BEF648C03920B0ADDA51261789A8E0B74FEB5F842B6C1C0542
SHA-512:	DA1365CEC6D040889B5E2F5368F7618360B437E4A009B3BF652C9D2CDBE899A42AD7BC6B6FB5921FAF8D0C40FDF27AD0A8921F828F7A3224D9BF053D8A84F07
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...:.....<...=...>...?...?...?...@...!...B...C...D...E...F...G...H...;...J...K...L...M...N...O...P...Q...R...S...`...V...W...X...Y...Z...]...._.....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 15:45:53 2022, mtime=Tue Mar 8 15:45:53 2022, atime=Fri Aug 12 02:11:11 2022, length=2203257, window=hide
Category:	dropped
Size (bytes):	1114
Entropy (8bit):	4.5747997284727475
Encrypted:	false
SSDEEP:	12:8EA/Cu0gXg/XAICPCHaXRBktB/eLX+Wx/xgiL9zwcivbeXNq9zwDtZ3YilIMMEpx3:8EAu/XThOm/fxLBTeKXkBwDv3qYu7D
MD5:	B6FF60C16AEC12E2FEF67851C9710167
SHA1:	4EF1CD47DA472ED93D512D1150892FB44F965DD3
SHA-256:	F4945108F532B4F9DE74B78D00DE4B23930262D3C96B8DE3FF68ECBDA6CC069B
SHA-512:	298974346AACF77CAEBF79D34ECA3ED7EFE74EFE3AC8C5726A1D726766029795F07B45C70E127A9A80D77A992A10AEDF8DB8E98DA0A4233D0E33CE9EE6629F4D
Malicious:	false
Reputation:	low
Preview:	L.....F.....P...3...P...3...y.!.....P.O. :i....+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.y.!..Uf. 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\.#.....\472847\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.

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):	111
Entropy (8bit):	4.815919561621978
Encrypted:	false
SSDEEP:	3:bDuMJleUHELgLplbUmX1bWEHELgLplbUv:bCU7Dbuu7Db2
MD5:	A649133664619D3CDC98418B3EC97D2A
SHA1:	0F597DDC41928FBB93544E5972B07D14365B386F
SHA-256:	3C7978588FF30B4B1BA90073AC13363A73058CAFB8F79B4189CC541283D07D75
SHA-512:	C819B43C5B49FF8D672525C903F2765ED7974D6CF017A6E5860C390D50A01946AF62A123FD5E1E98672A96901DC55E9DCFCAE2F880780653C27EAFB736201A6
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..cis-broadband invoice 08.11.22.LNK=0..[doc]..cis-broadband invoice 08.11.22.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:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/I
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD68A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDF533BC9E428B0637562A6A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.I.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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFD1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~\$s-broadband invoice 08.11.22.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:vrJlaCkWrVyaJybdJyIp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/I
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB8BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562A6A
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):	7.993383170496904
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:	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:	FAB53374AA4EC9D32EA4FA3B1D78634E5F6C97C8D30B84657671F1902D0AAA1E03E21F5
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...<_.

File Icon	
	
Icon Hash:	e4eea2aaa4b4b4a4

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

OLE File "/opt/package/joesandbox/database/analysis/682661/sample/cis-broadband invoice 08.11.22.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: 2837	
General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2837
Data ASCII:	.h.Attribute VB_Name = "ThisDocument"...Bas..1Normal...VGlobal!.SpaceFalse.JCreatable.Pre declare..Id..#True."Expose..TemplateDeriv.\$CustomLizC.P....D.? PtrSafe FunctionLib ".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..Name="Project"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="EBE9F817E71BE71BE71BE71B"..DPB="D6D4C50C5B1C471D471D47"..GC="C1C3D2D7D3D7D328"....[Host Extender 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 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

System Behavior

Analysis Process: WINWORD.EXE PID: 2032, Parent PID: 576

General

Target ID:	0
Start time:	20:11:12
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:	0x13fac0000
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	6E132B14	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF1CF4A488C21180D9.TMP	success or wait	1	6E1B0648	unknown
C:\Users\user\Desktop\~\$s-broadband invoice 08.11.22.doc	success or wait	1	6E1B0648	unknown

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

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

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Fonts\StaticCache.dat	unknown	60	success or wait	1	6E4AA0EB	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	6E0A1925	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	6E0A1925	unknown
C:\Users\user\Desktop\pcis-broadband invoice 08.11.22.doc	1871659	184	success or wait	2	6E1B0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FAAE737A.png	0	65536	success or wait	4	6E1B0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\83C87933.png	0	61935	success or wait	1	6E1B0648	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E18A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E18A5E3	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400100000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358626865	1426784306	success or wait	1	6E0A1925	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	6E0A1925	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	6E0A1925	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	6E0A1925	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	6E0A1925	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	6E0A1925	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	6E0A1925	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	6E0A1925	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\78CD4	78CD4	binary	04 00 00 00 F0 07 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 F0 07 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 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 00 61 00 6C 00 5C 00 54 00 54 00 65 00 6D 00 70	success or wait	1	6E1B0648	unknown

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

FF

Disassembly

 No disassembly