

JOeSandbox Cloud BASIC



ID: 682678

Sample Name:

beyondsearch,doc,08.11.22.doc

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 20:30:24

Date: 11/08/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report beyondsearch,doc,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\9F7E4C0A.png	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D8AFD883.png	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{67659BF2-E797-4523-855D-8CB155CDBA2F}.tmp	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{700A5179-F871-4510-B8B1-F8AE9A6BE9FD}.tmp	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{803ED0A8-1C9F-405F-9890-D3A13AC7DC84}.tmp	11
C:\Users\user\AppData\Local\Temp\~DF396E86B8EC924EF0.TMP	11
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\beyondsearch,doc,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\~\$yondsearch,doc,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/682678/sample/beyondsearch,doc,08.11.22.doc"	13
Indicators	13
Streams with VBA	14
VBA File Name: ThisDocument.cls, Stream Size: 2802	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: 485	15
General	15
Network Behavior	15
TCP Packets	15

Statistics	15
System Behavior	16
Analysis Process: WINWORD.EXEPID: 3000, 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

beyondsearch,doc,08.11.22.doc

Overview

General Information

Sample Name:	beyondsearch,doc,08.11.22.doc
Analysis ID:	682678
MD5:	ab5796d82e0a84..
SHA1:	3e69850c66255b..
SHA256:	500b85d4e573f6..
Tags:	doc IcedID
Infos:	

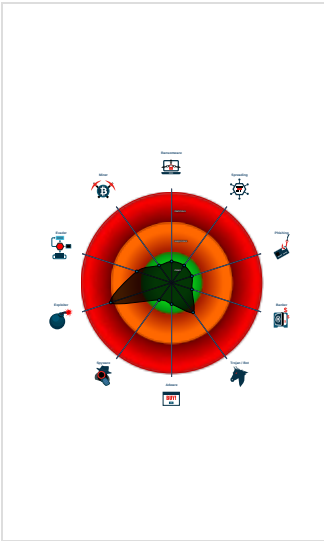
Detection

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: 3000 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



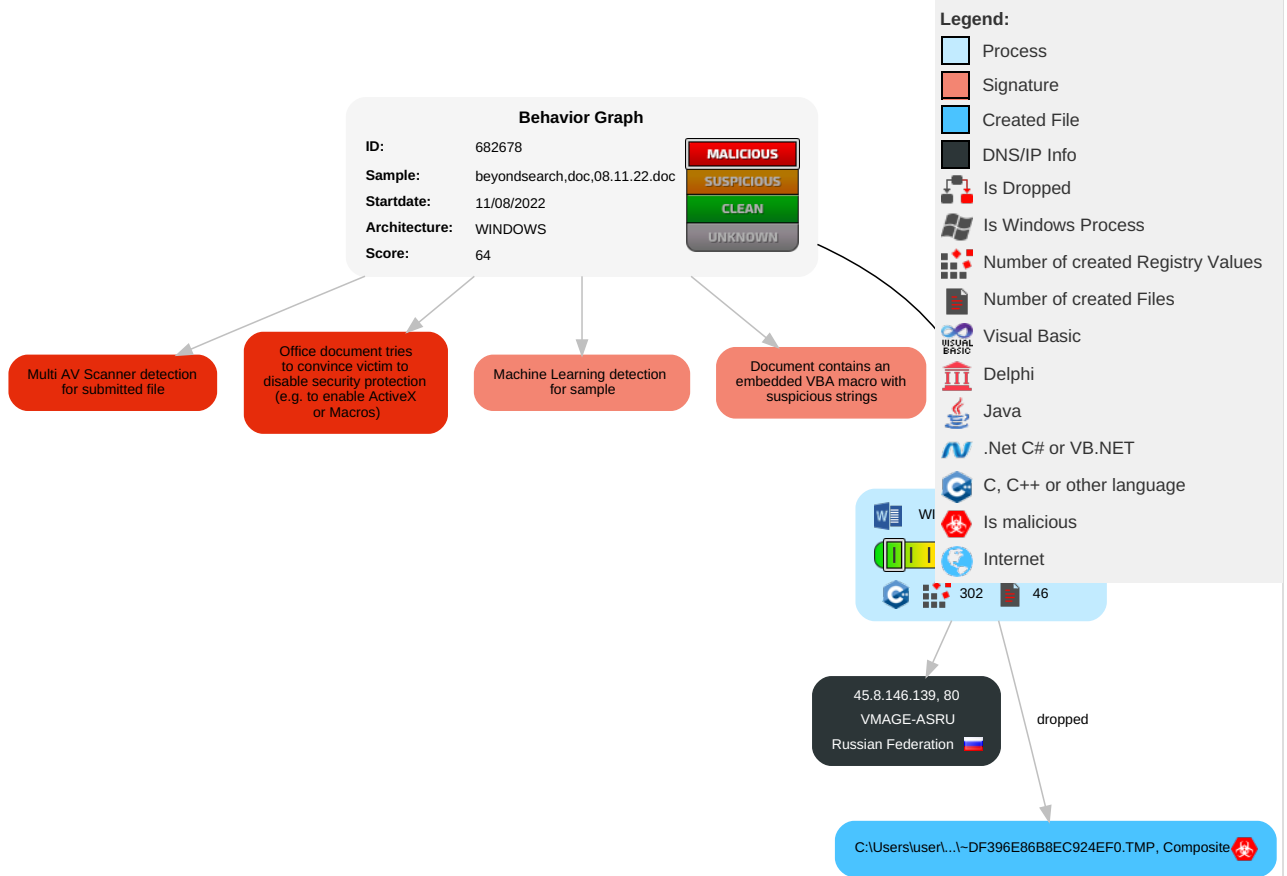
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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

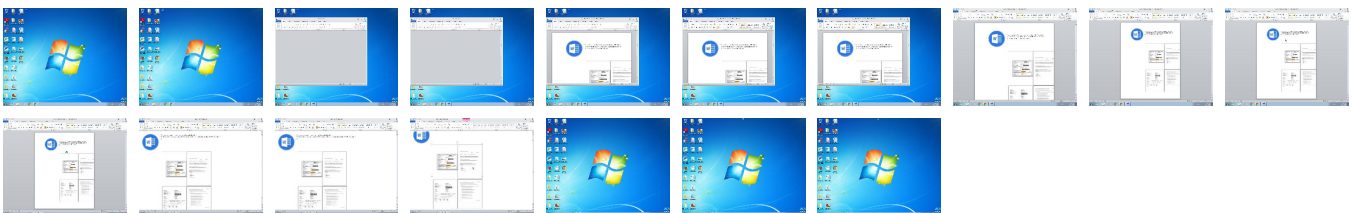
Behavior Graph

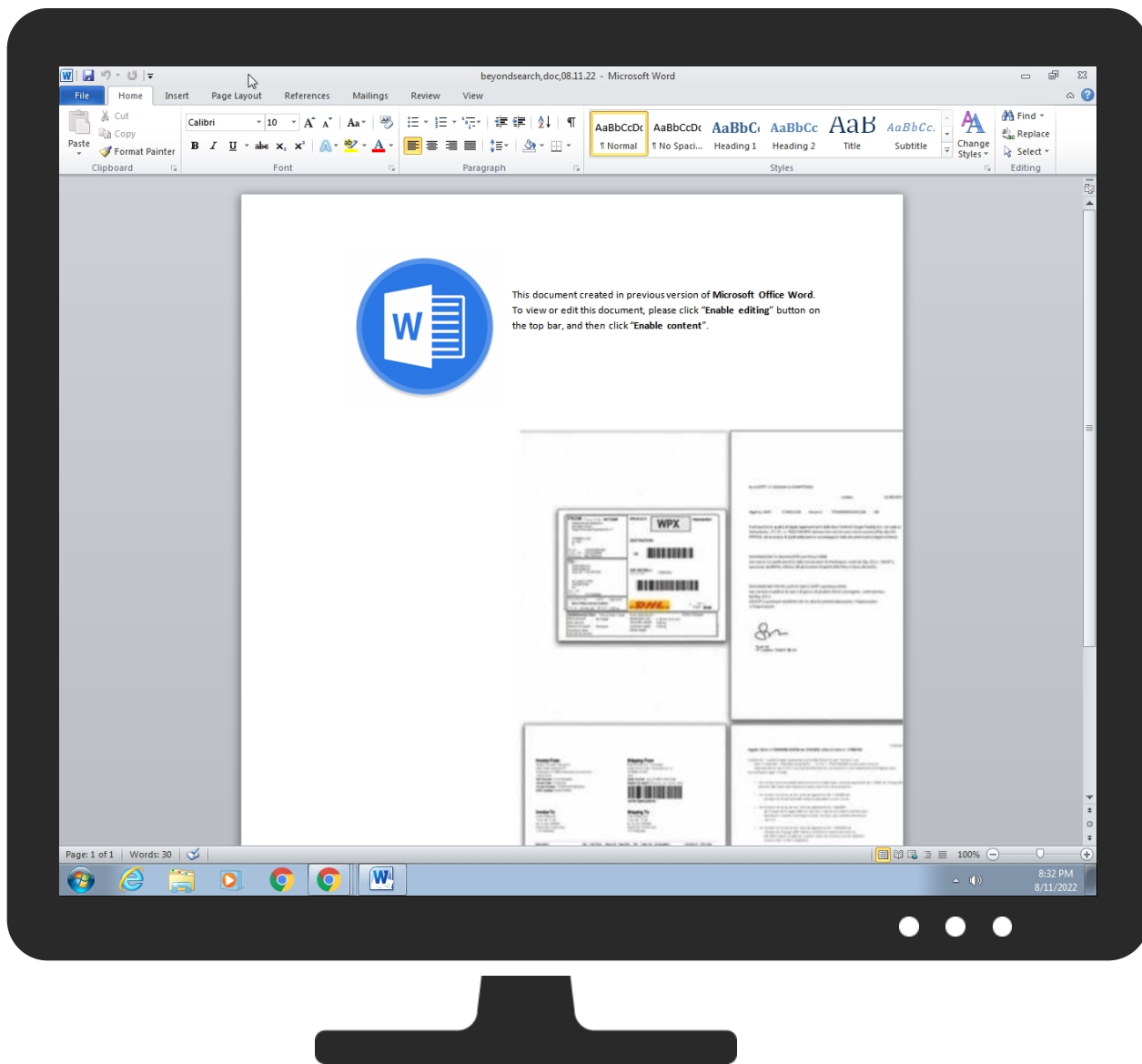


Screenshots

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
beyondsearch.doc,08.11.22.doc	23%	Virustotal		Browse
beyondsearch.doc,08.11.22.doc	15%	ReversingLabs	Script-Macro.Trojan.Amp hitryon	
beyondsearch.doc,08.11.22.doc	100%	Joe Sandbox ML		


Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF396E86B8EC924EF0.TMP	100%	Joe Sandbox ML		

Unpacked PE Files

 No Antivirus matches

Domains

 No Antivirus matches

URLs

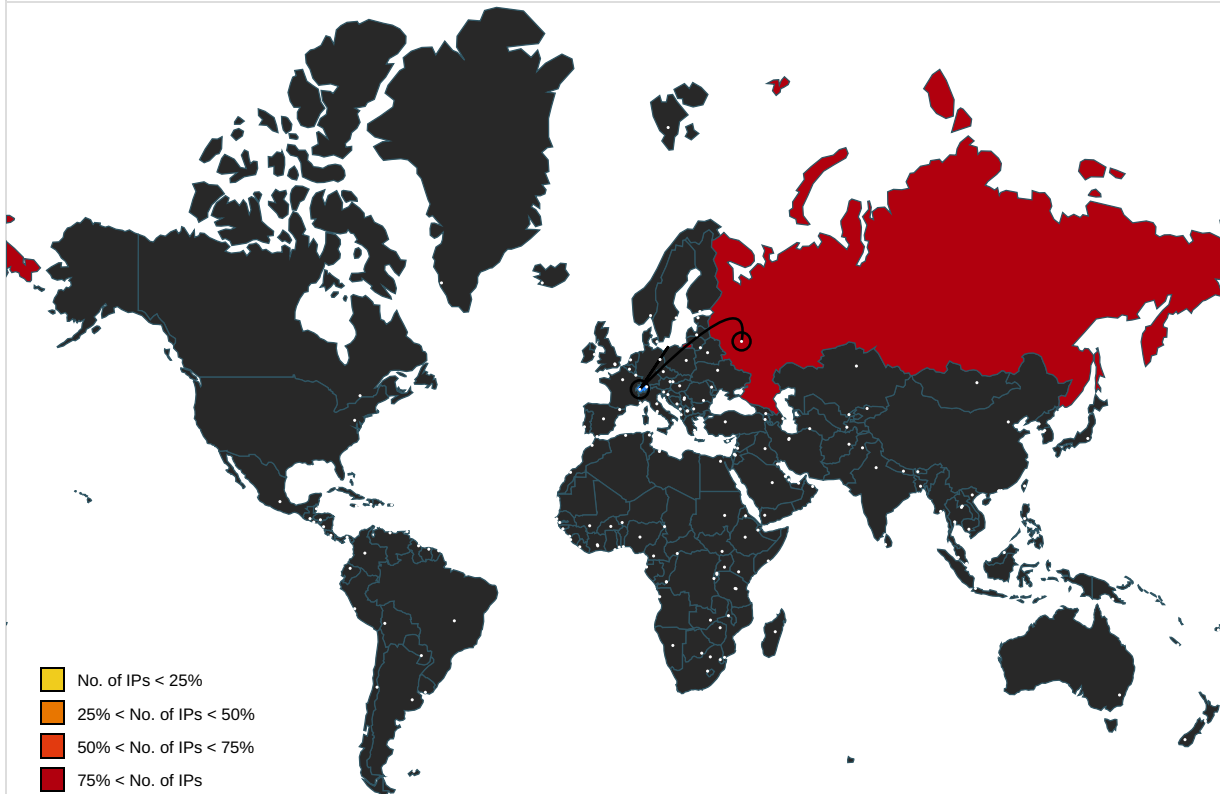
⊘ No Antivirus matches

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:	682678
Start date and time:	2022-08-11 20:30:24 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	beyondsearch.doc,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\9F7E4C0A.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):	256276
Entropy (8bit):	7.977216150398352
Encrypted:	false
SSDEEP:	6144:u53FFY/qeTrhmcfFRbmQbtjZXZkMDX9YhHa0MeIHuE+1wp3OOaEKwOYojl:Fie8cffRb9njZdmw0fSuchOMKwEJ
MD5:	7868B0F9CF2B7A4AD1CD14D32F5AD036
SHA1:	745B716D2061FC543F3511B9391CC590B5B2B7C8
SHA-256:	9454CDF04F8BA921663CAC8DD825D4E8602FA4BAC4DBBD775267A5949B41B83E
SHA-512:	A7E764CFDF6FED1445E618FCCA6151B75FE20C06F99C9FA7819A6CECBB7E5F3FBC61979A8E511D84E44ACE0FBCC899F04D0069D79F007CD62DD62BE1A14309
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs.....!.....IDATx^.....GU.....]g.m....?J.....(....5.....@.B....lzO:!.H#a..3.=.....!CB.....~.....w....J]....K....S.UuNU]u_.O.w....~x:0.?+....K.x.{..6..N..o....A...p....D/_+..i..x..o<..[so...A9~A8....*p:P.=Z...X....x[Z.c<l.....VF..'..6.....ic.l.[....._2.h.J....6.K....N.>...p.+~...x-~_i).W..<..L....J.8 . =z...hy+.A.WT.[5.....g....ct.*O_[.E..5.2....>...h...c.0.....~E..z.*.....*_.....'r!\$...m].[5..g.WN..A..[i="i..x...p...~.....V..@...z!...@z.3F.8. u...A+_E.W....5.HZ.U.b.x....x..1+...D....xvF.....@.h.a.'.)]...~_.h.Z.V:h..l.....E.N..u..p..5....{..x..6o:'-...%z4.4.\$.....*jz....T.qP.U.ZZ..X..k.Tz.?@..6...~...s..g...^..W.b...D.....%j..y .O.....~F@....k.A..7..H..."@.'!'.h..z<pOFM.....9.i..m..1..U.h....1Y..v...r ..z/8...@...O.O.U..ymz..._]E....j Vc.6...^..X<yq....1?Q...jy.....b.?]...l~D..... y.6.*...D..



C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D8AFD883.png	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 486 x 628, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	106990
Entropy (8bit):	7.9875389343574765
Encrypted:	false
SSDEEP:	3072:BTmfkQHtM8ZGSnYO7/MCGQGzM/KsDN3jBU8zq:BTmsQNDGSnf7/CQGz6NHq
MD5:	003B5C109509AD99FB418712CB4B184D
SHA1:	145B7864A0CE5E0CA42AA6DDCAF2E3B5052071C9
SHA-256:	131B8A928D925E1A7EAA188384BD499856749DB1523D310516079162CECD2368
SHA-512:	3F0B828957260AE725A0EAC0FEB4484D76F398EDB31FBF10AC9797D7ED66D81F24F34D0986CE6DBFB92C07919AD18D9773704CF3CB3D35015C69F5DF2FC4658
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....t.....H..M..IDATx...\$u.#k.z.gDS.\$0.....`..aj.Lk.h.....>...].N.0.h.Tg..y....q.n1...Q..O1ny.. .)...b..].9Wp.m].u..9.u..E..u....o...M8..?.8vQ..._../#.. ..5G..7r.S+.n.Blr[s...9...B.....8t...\.6....._a.\$...v...v.8.y.s.....1.v..1.t.J.(#..q.8...}.N...z..B!l!;7.f.+D1w.v.8rQ...l+...b.q..E.(^.....8...>.P.s...?U?.....(.....U.....f..0...s.P(DQ.p.P(\$..f..6..B..n.....(.QT.....(*....R.E.(.....QT_.....).6"...v..l6...Y....r\2..5...b..l.....{.....m..8..Q..c.@.D.bT(D..];....8J.yq.....'+.%..C..E..35...&g...xc.7.)*...m....l6....b1S...B'.o8K.?_O. .R.....W..B.._..^....>...b..\.Q.....(.....h.h....Pv).h.E..v.ZM...l.Z..8.?y...%.....%....bT(..1.1*.n... Q...E.Ba.o.....M[2.l.#...Oa....x... z....3.b.l_.W..p8....f.ab..6..v..~..&m6.....+&...S(..R...v.._W.t.Q..h[.ly.~.....T*q.^?B...Dm..b.X...~8.>q.....}...7...E.v.....s'..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{67659BF2-E797-4523-855D-8CB155CDBA2F}.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):	11776
Entropy (8bit):	5.802602301153295
Encrypted:	false
SSDEEP:	192:yktJ6pa/Rr3pmlxSE4kHapt3mpa/Rr3pmlxSE4k9a:/tApcjMxH4zt2pcjMxH4
MD5:	0346203C08BC40A669A667D7F7F1CDA4
SHA1:	29CDCBB2B4672E652B553A5CFA4F6913E05294FE
SHA-256:	A52FAE14F6E1F888A54038E10EAF43B4FF1A9B4725112AE9446434B668422342
SHA-512:	F94C51987173B97B783D151E85F9198C57A3CEBFE9095CC3A4157F253C99BDAE37FFFE6B348510A3701982CD3BAD5FF39307770FD86611A256A77523EDE31774
Malicious:	false
Reputation:	low
Preview:>.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{700A5179-F871-4510-B8B1-F8AE9A6BE9FD}.tmp	
---	--

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.1213119425347764
Encrypted:	false
SSDEEP:	12:DMlzfRLRW4WZ1MFKuQ9cc3xn82l6kwkvjTS4BTFkYW4dkYW4PIlWkYWHkUzB/Wz:4LG1ND9Pxn82EkRSCFmUmYImHWz
MD5:	6092D6A6540809400150272965A545E9
SHA1:	3C783F523AC30DE7E3A25D67BE70C578846E9ACD
SHA-256:	EE62AE57659119FA9069F589F2B235189902CA53535FBB7D852755D5AFA0B39D
SHA-512:	44E6E8DB919FFA15BD860B7B1A91AE61351C37C5F0F7EDA5B22EA98C87629622EBDC0FB216E21B1C7BB009850E2EC01F5FABDBE6C5C4398DEAA0695B18B78844
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{803ED0A8-1C9F-405F-9890-D3A13AC7DC84}.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:	95F83AE84CAFCCEDE5AEF504546725C34D5F9710E5CA2D11761486970F2FBECCEB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:

C:\Users\user\AppData\Local\Temp\~DF396E86B8EC924EF0.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):	59904
Entropy (8bit):	4.163773817291896
Encrypted:	false
SSDEEP:	768:VdvVZwOTx6iJ1TVMT05lrzjs36EdX17+Mhd72+ajLGIMG+aGXaD3:VpzT0yAT0rzO6EdX1L0GK+aGXaD3
MD5:	220BF14C27C7F30EF3122CEDD81CC3AD
SHA1:	842967C6E66C823E45DDF93E404C53090A088699
SHA-256:	34A03251C9F48854545A74505BD30B9289377DA8C4E2C48793364B7525ADA1FF
SHA-512:	05F026CDB3B7927C423BB36A10264A4A70FC08E2707CBAEEB7D270BBE935A8C290DE9CB0F963FAEA79C24C9EE390AD07DA7B2432D82FEDA5E604B94C888555BA
Malicious:	true
Antivirus:	<ul style="list-style-type: none">Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:>.....S.....(.....!...".#...\$...%...&...'.....)*...+...,-...../..0...1...2...3...4...5...6...7...8...9.....;<...=...>?...?...H...A...B...C...D...E...F...G.....I...J...K...L...M...N...O...P...Q...R....._...U...V...W...X...Y...\. [.....h...^.....a...b...c...d...e...f...g...Z...i...j...s...l...m...n...o...p...q...r...]

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\beyondsearch.doc,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 15:45:54 2022, mtime=Tue Mar 8 15:45:54 2022, atime=Fri Aug 12 02:31:13 2022, length=2248938, window=hide
Category:	dropped
Size (bytes):	1089
Entropy (8bit):	4.559456310102049
Encrypted:	false
SSDEEP:	12:8cZuvgXg/XAICPCHaXBKbnB/xQpX+WqpWaiKit4icvbnnp/l4bibDtZ3YilMMEpn:8Z/XTRKJlwpWtKWred/EmDv3qTau7D
MD5:	8BCCBE98C6A0A6031F43D2C66E22E5F5
SHA1:	44ED0D796B3155DF1592AC984E89785C36454DEB
SHA-256:	4A815A75BF204F31D8E7D2FABB7EF83F76CFFA6916FE07EF23198C92EC195600
SHA-512:	54F2D3E6D04988E32A0AE35B1D78BB1C897FCB89F0B7160CE331ABB7206A34DD4E9B200F06ECC6ACD90A53EB8AED6ED5D394468F58C92B80A93586E5875FE455
Malicious:	false
Reputation:	low
Preview:	L.....F....UU..3...UU..3..N.....P".....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.....2..P"..U.._BEYOND-1.DOC..h.....hT..hT..*...r....'.....b.e.y.o.n.d.s.e.a.r.c.h.,d.o.c.,0.8...1.1...2.2...d.o.c.....8...[.....?J.....C:\Users\..#\.....\\116938\Users.user\Desktop\beyondsearch,doc,08.11.22.doc.4....\.....\.....\D.e.s.k.t.o.p.\b.e.y.o.n.d.s.e.a.r.c.h.,d.o.c.,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..

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):	101
Entropy (8bit):	4.744445088413295
Encrypted:	false
SSDEEP:	3:bDuMJIf5K1HEKpdJVJUkUmX1SHEKpdJVJUkUv:bCUU1HEKVJVJpbWHEKVJVJpb2
MD5:	56105FFA4A3B63A6FC6A6DA6E8650B6B
SHA1:	AB9CE29AAEE1FCEC81C30A703C6F5FA946ADAD96
SHA-256:	C4786521292D9F0EE34406B886128FFDF8F76F8A0F91A309FC7DCA0F90849A0D
SHA-512:	3DD4584DAC93664700B740BBA2CECD2A7DA7DDD0750A668B8E3E1DA16362E6B0922A2377175C0C568134C06597BC4246DE73C25EDC3DF4AA4B1DEB1AD07D15B4
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..beyondsearch,doc,08.11.22.LNK=0..[doc]..beyondsearch,doc,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:vrJlaCkWtVyHH/cgQfmW+eMdlN: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...

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\~\$yondsearch.doc,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: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):	7.993497837774047
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:	beyondsearch.doc,08.11.22.doc
File size:	2343139
MD5:	ab5796d82e0a8467837ced35e6b725b7
SHA1:	3e69850c66255bbd093579fdb161a16e64d8a848
SHA256:	500b85d4e573f6e14e96c0a06e2d8fe15572c0eb97e3cc6d204d3416140d8a61
SHA512:	20c4a3d6f701eaebe2b201d29ac9939484bf8e72e57cdf5f82c99d1bb04f2bd3a9a488dcd901ff0facc2542e9b7a15df0c0a715de32f6f325bcb6965d76135
SSDEEP:	49152:z/hO6rfJ7OgTHnzfRPGPNJvF3620rpD9wpZF7R:z5JQgDnKJvF3620NDOpdf
TLSH:	BCB533FB81555325D1E33E7DCA6BD2CE8C4AAACE252EE404AD1F4F84CF129C4756AD0A2
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/682678/sample/beyondsearch.doc,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: 2802	
General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2802
Data ASCII:	.p.Attribute VB_Name = "ThisDocument"...Bas..1Normal...VGlobal!.Spac.IFa.Ise.JCrea.tabl. .Pre.decla..Id..#Tru."Expose..TemplateDeriv.\$CustomlizC.P....D.?PtrSa.fe Funct.ionLib.."user32".Alias".KillTime.r"(ByVal.....#.As Longy5, ..
Data Raw:	01 70 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:	5.25516442275755
Base64 Encoded:	True
Data ASCII:	ID="{5E1FDBD3-EB85-4903-95D5-63F3500ECE7E}"..Document=ThisDocument/&H00000000..Name="Project"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="434146058D098D098D098D09"..DPB="868483CA854EC94FC94FC9"..GC="C9CBCCD1CDD1CD2E"....[Host Extend er Info]..
Data Raw:	49 44 3d 22 7b 35 45 31 46 44 42 44 33 2d 45 42 38 35 2d 34 39 30 33 2d 39 35 44 35 2d 36 33 46 33 35 30 30 45 43 45 37 45 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

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

General

Stream Path:	VBA/ __SRP_2
File Type:	data
Stream Size:	5108
Entropy:	1.9294791789834775
Base64 Encoded:	False
Data ASCII:	r U @ @ @ 8 P " q A ` ` l #
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 00 00 00 00 00 38 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 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 a1 07 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:	2.706701541324898
Base64 Encoded:	False
Data ASCII:	r U @ @ @ x P p A ` q p q 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 00 00 00 00 00 1a 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 78 00 00 00 08 00 50 00 c1 08 00 00 00 00 00 00 00 00 00 00 00 04 70 08 00 fe 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: 485

General


Stream Path:	VBA/dir
File Type:	data
Stream Size:	485
Entropy:	6.301314382548745
Base64 Encoded:	True
Data ASCII:0.....H.....Project.Q(..@.....=....l.....Zd-...".<....rstdo.le>..s.t..d.o.l.e.(.h..^. *\.G{00020430-....C.....46}#2.0#.0#C:\Win.dows\sys@tem32\le2..tlb#OLE. Automati.on.ENor(malENCr.m.aF...cEC.....m.! OfficgO.f.i.l.cg..g2DF8D0.4C-5BFA-
Data Raw:	01 e1 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 e1 5a 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 20:31:24.003114939 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 20:31:27.020700932 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 20:31:33.027293921 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 20:31:45.046876907 CEST	49174	80	192.168.2.22	45.8.146.139
Aug 11, 2022 20:31:48.051424026 CEST	49174	80	192.168.2.22	45.8.146.139
Aug 11, 2022 20:31:54.058000088 CEST	49174	80	192.168.2.22	45.8.146.139

Statistics

 No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 3000, Parent PID: 576

General

Target ID:	1
Start time:	20:31:14
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:	0x13fb50000
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\~DF396E86B8EC924EF0.TMP	success or wait	1	6E1B0648	unknown
C:\Users\user\Desktop\~\$yondsearch,doc,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:\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\beyondsearch,doc,08.11.22.doc	1872000	184	success or wait	2	6E1B0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9F7E4C0A.png	0	65536	success or wait	4	6E1B0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D8AFD883.png	0	65536	success or wait	2	6E1B0648	unknown

Registry Activities

Key Created

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			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\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1358626844	1426784285	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	1426784285	1426784286	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	1358626844	1426784285	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	1426784285	1426784286	success or wait	1	6E0A1925	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\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\7A850	7A850	binary	04 00 00 00 B8 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 B8 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	6E1B0648	unknown

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

FF

Disassembly

 No disassembly