Joe Sandbox Cloud BASIC

ID: 877007
Sample Name: Contract agreement.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:15:36
Date: 28/05/2023
Version: 37.1.0 Beryl

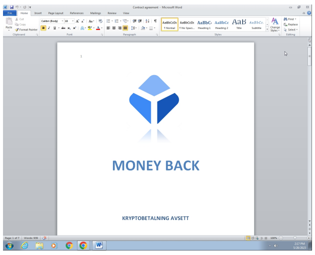
Table of Contents

Windows Analysis Report

Contract agreement.docx

Overview

General Information

Sample Name:	Contract agreement.docx
Analysis ID:	877007
MD5:	494ad369620d..
SHA1:	57c451f3c0af7…
SHA256:	2390662435e3..
Infos:	
	

Contract agreement - Microsoft Word

MONEY BACK

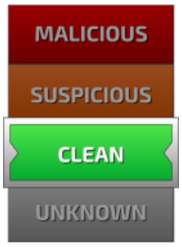
KRYPTOBETALNING AVSETT

Page: 1 of 7 | Words: 939

100%

2:17 PM
5/28/2023

Detection

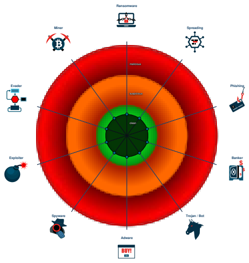


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Document misses a certain OLE str…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2188 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

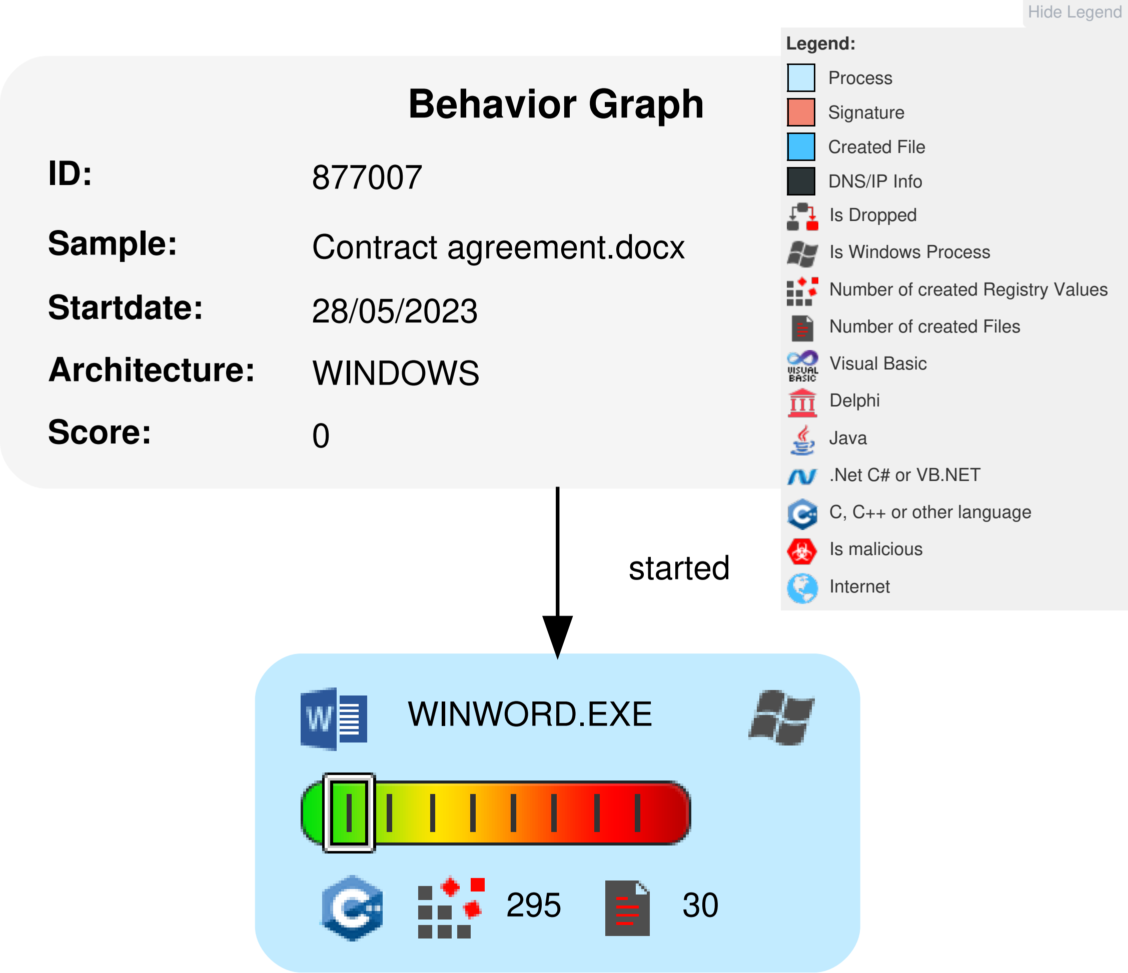
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

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	Windows Management Instrumentation	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	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	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

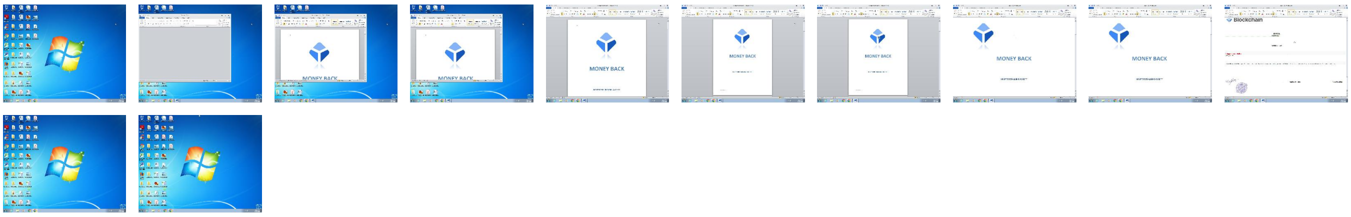
Behavior Graph

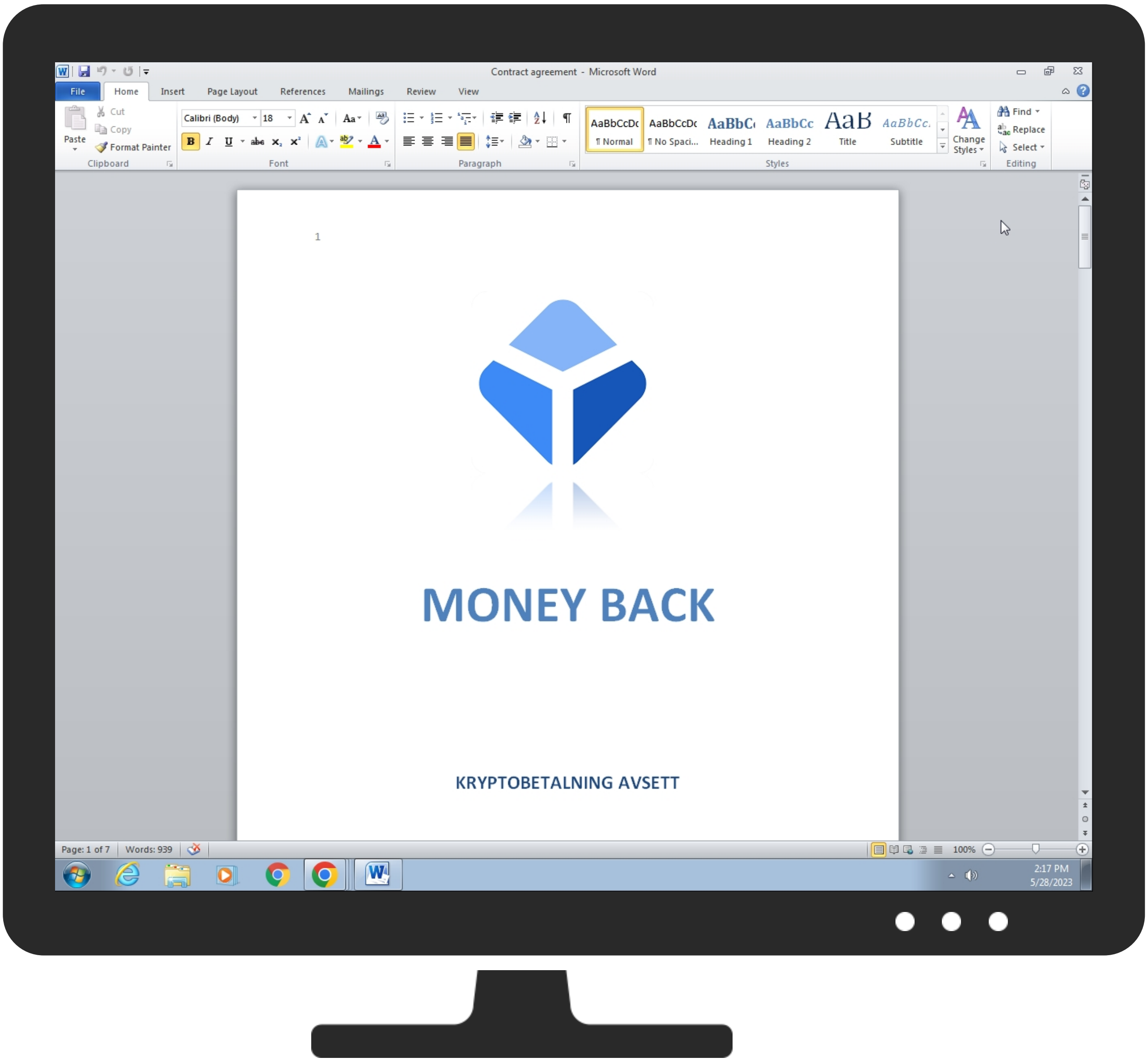


Screenshots

Thumbnails

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





1

MONEY BACK

KRYPTOBETALNING AVSETT

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

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

⊘ **No contacted IP infos**

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	877007
Start date and time:	2023-05-28 14:15:36 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	2
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	Contract agreement.docx
Detection:	CLEAN
Classification:	clean0.winDOCX@1/13@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .docx • 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, t oo 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\2BB8ABC6.png

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 1054 x 274, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	12033
Entropy (8bit):	7.814046314403372
Encrypted:	false
SSDEEP:	192:Yo6IjAHr7WP4702cGwLM3nYQYHtbi+YssYWs5/OryMSHgg4QvuG6Td3V2Sa6Vti:WbHr7Wk09inYfHtbi+YuOGMygg4V5dE3
MD5:	1982F2115020E93B3AAF65C919E5E7B1
SHA1:	8E4AF970E33E083E62FB1D9FA709C59E876FDB23
SHA-256:	B310B9D089845E82397A55AF32151F3A20B7B20AE6634C84C3B03B0267DAE9F9
SHA-512:	269BDA663C90B7454F942615ACC283CC4D0DAF292E1BAA430593ADE534B8007AF430FFB66ACE0AABFDB2B9C4F6A880703FA12B82112D45AB86757CF54A5C81 FF
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR.............Z\......sRGB.........gAMA......a.....pHYs..........o.d....IDATx^.._.e.}.p.I.L.XQp"gp.pjI...B.8.P.,?.B.k.!!.1C...}q!c=......`l..Pj.N....y.B\..n.B..-..4.8J...Vk...WZ+:..3s.9{......}Fsu.>k..w.....y..{.....x].....`p..................hF.....4#x......<...........f.....@3..................hF.....4#x......<...........f.....@3..................hF.....4#x......<...........f.....@3................hF.....4#x......<...........f.....@3..................hF.....4#x......<...........f.....@3..................hF.....4#x......<...........f.....@3..................hF.....4#x......<...........f.....@3..................h..7o>^......7.?..o_....7.../...O|.W.(......<p.W^z....&H.0...~..q..}....u(/~./%..B...0E...}./...l8j.p....~........L..a$.V8..7}...o{..*....F.0........DYmB.....S...ejE..!RI...z.J...........{....>$..>...0..C'.C.M.....W~.....@7.......?z.............M!t.T>.....)........z.8.F..:l..._..~........t..SO=|...7n.8Q........^..{.....3'xh`.C

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\93279D0F.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 367x226, components 3
Category:	dropped
Size (bytes):	16041
Entropy (8bit):	7.908036013679057
Encrypted:	false
SSDEEP:	384:UJiwuzBzGFGiGn0Lo5x06rJJFQc/eDlLyT6iQp:UyzBMTGn0uRJJmc2hLs6iQp
MD5:	532ECCFDAB55D04C4A1F0C74DCE69AC0
SHA1:	082C285DF47E0FA97DE967F8FF44DF12962384DC
SHA-256:	CB024CFF62003E835785C68BCA97A29818DFF1FE58F46C91D5B6BF889752F951
SHA-512:	D9A4150EF19A6CA2B3A73E6FE0625C5F1C56B4D6365BBD2816A12D8EFF7F448D69855B9B1413BF07594A93757915FAC43D8566ABBF5DAEECB5FC87EAA5627D 66
Malicious:	false
Reputation:	low
Preview:	......JFIF.............C...C..o.."...}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..?.....l..#)..1..:...[lEU...rq....(.9..u ..1..R.m....m_JZ(.....?.R..R.P.I....ho.2....F(.....4..).&...."..E.P.b.D...InNz.N...(..,....(...Z.(.....?.....h.6*.<0-.B..^....H.o.\...3H.VDV...g..ME.[..}B.(....E..Rm..P.E.P.E...P.E....(=(... ..4...3E..W=......Y..B..m..R...=z...;T..j.P9....m.Q@..P(...sHI..h.i.w..~.....z.E....K@......@9.f.....QE...(...(..#..K.Y&.p....)c.2x

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\980DF3C4.png 🔒

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 280 x 239, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	123518
Entropy (8bit):	**7.994272940906965**
Encrypted:	**true**
SSDEEP:	3072:/NuCUlIjWXRhoC0Sf9bHpUHgl7Ms7EWyljC/o6fvD:/rE9Z4gRMNW1/r
MD5:	6432EC45A44A1CE70C6D31D7910B3D8B
SHA1:	8BC88D78CB0231AFC15BE30E292A0663411C8624
SHA-256:	60AB53BD284207BE4197833C4F8B1632F860BA0183C52C9B8E0608BCED63BB14
SHA-512:	4F536E910627D7D6BF4D9D2F43E08BF5E85536C2FA55B531640D589C323B25C74EA9BA79781799036DF014B2C5CEFF6AA9DBFB4844FF6FF2F7D2C248970890B
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...............\.....sRGB.........gAMA......a.....pHYs..........o.d....IDATx^...`..?..Y.]i.+ff.,..L...i.&m...I..I.h.@.N....eK....+.....r....}............{.=.s>.....y.o..a....}...C..5....q..7.... <.u...F.A4...-s..i.....~|l...w..$::.pE...U...6.>~..%$.45...v.qR1..c......5....\.388......[....;..6zz.z.W^|O......<..aA....9o.5... E....D...5 .7.Y.h#'4.&.= .o,.........o...'+.j....O.:..o..F..q.3......- l.c..0~..%..T.jy.9hD...u..o../O.4.....](...........z...EK.,......NHL.x{PP.....8.4.2..;oK.Z:TTt.'vTW.GF.....Q.....Z........V...k.9?".....8E".+.x...1=-.8.R.kLQ..\.n.7.Y.J...............~.F... ..._\....Lnv.`....^..Nb;.Fg...E..[.....}xxxEu.O..+WFG.`.... }[k.F.JI4...E....[..e..i...............O..t.$.....R.....=..(....J*G....Y.9...}.....]*...o....O.t...U.3.}....qc^C.c..bB........A.?}JjLR..0..} .g.F.....wD.k.o .g.j.>.W.8D...).....lA!...{.=Pn6.>.....+I).)I>p..o.$..bZR..v9.,Jx.......4.#.3.7H._r......2=.....5S..q.R.....|........Fo..BHA!R.%.g

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E287E699.png

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 225 x 225, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	1872
Entropy (8bit):	7.820973115519834
Encrypted:	false
SSDEEP:	48:rZD2m8v+zT16rTGv6bYOx4cicaV2fs6QV4oJX:NDjzTYrRYupvaEs6roJX
MD5:	3DDCCDFCD959C07AB9A2F7778923DFB9
SHA1:	D6D40BC9AEF8DB200A9612B7D5794E3CE3FAACE1
SHA-256:	E701C4434517707206E3DAD5D1E84249B423F0C932B79F1CE71E434B227D6240
SHA-512:	D8BC7418C461B81FBC20D7D3BCDFC4EB22E76CEAD6391049D6363DD4909EC2770BE024BF73395097090C514C245C91730C01B5BDA886BB6B6FB8B4085B7C3C 9D
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR..............m"H....PLTE......=...V..O.4...........{..9...S.(.......F.............Y..6g...........A..J.....D..@.......N........@m..}....k..Ov...............E..........u..|..c..)_....lt.q..a...b ..R_6...ZIDATx...m{.6..`.8).).....H.u.ei.u....a....D...*......:..@..O.>}....').j>.I..U.}$.i...?......r>...;....Q.e:..=!.S.#.....{4..... ...kSo......[..2^.}..v...C.Dd....Z.1.X01.X,1.X(1.X$1.X 1.X.1.X.. .,....D...!...1.".8`.D,.N../..9.).YO.i..7*.0.F..f...,....a.R..kTz`f....Qy..5*.0.F..f...,......T'.....@U..P.(.T#.....@..,P.(..'.....@Q..P....#.....@...P...d'.....+ub=c.n.w.Fv..Q.h...]P0.....> ac.VZ..2.....>.........1._.z.8+_.3R..f.kCg....h}....y.............J.......U....xG.t#....rt.....d0.3.|...(.......Y.q\.|6..g.....N|..6..R..@N#./....e....]@.#./...9..Fz_,...4..Zb.M...TF..........@.#..%.. .q|....0...X.o.#|6..Cc.}...../...\..Fy.."{..h.../.a.O...:r..>..7.m.B.hL..T..RJ(..>[.O..n.J(SG..~....&......,..m>D\...2B}....s........w..l......\.;..f..s....../1>+..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{60BF3DE8-1CA3-42CB-B6CA-E671C80F0F56}.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):	2560
Entropy (8bit):	1.4200733097516376
Encrypted:	false
SSDEEP:	6:rl912N0xVN+CFQXeDXw9XfA9XfA9XCw9XfA9XfA9XCw9XCw9XCB9Xh9Xh9X:rl3lTpFQgXIwwCIwwCICICb77
MD5:	2ED4F5AEFC83840D2981F9ADC2F6460D
SHA1:	8AE268AC0E0B730B7973FF0485E689B52E483FC6
SHA-256:	A34946B2D938BD91DDB4B6E06B495F575BED87EEC17764C9EDD5D0A7DF5995C6
SHA-512:	618E5F60F3DA577B52ACDA47F1334CDDF8E3D89DF0A59611461D3D4D42212A355159DFACC14E37E713D3E1F5BA47771417E7354E23067E396E1420CD60E59FE
Malicious:	false
Reputation:	low
Preview:	......................>... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9D5B7132-C829-4FE2-85DD-9FE723688C9F}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Targa image data - Map 6 x 7 x 8 +4 +5 "\011"
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.9761180206469766
Encrypted:	false
SSDEEP:	384:plmL56u5fvg+e9Dsi3nI9Vp2SdkBg4GvGLuHUNLCLpecS8kPz:PKSTb
MD5:	A060B65BBA744CE5658560E8C225A469
SHA1:	296865DC3F3170AEE4DB1DAFC1BD00E1243E41CF
SHA-256:	A09917E33EDB7496696D6EDF38C56106B422BD70F637C935FF0A66656B940086
SHA-512:	A497618616CE8C7FE66568D7E0043D120AE58CEE2B5B71150D29D7CEAB6894CB699FC69E98B523800CB62BBC92F5FAC69BBEE915A5D5E1D47F5C454BF5577C F2
Malicious:	false
Reputation:	low
Preview:	....!.".#.$.%.&.'.(.).*.+.,.-.../.0.1.2.3.4.5.6.7.8.9.:.;.<.=.>................./. . . . .M.O.N.E.Y. .B.A.C.K.........K.R.Y.P.T.O.B.E.T.A.L.N.I.N.G. .A.V.S.E.T.T. ....L...b...d...f...h.. ....$...Q.^.Q.a$.gd.~.......$.a$.gd.VI... ...$.a$.gd

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{C7F1C78C-1140-4E43-A415-F39DE2B8E989}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\mso177.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

File Type:	GIF image data, version 89a, 15 x 15
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.949125862393289
Encrypted:	false
SSDEEP:	12:PlrojAxh4bxdtT/CS3wkxWHMGBJg8E8gKVYQezuYEecp:trPsTTaWKbBCgVqSF
MD5:	ED3C1C40B68BA4F40DB15529D5443DEC
SHA1:	831AF99BB64A04617E0A42EA898756F9E0E0BCCA
SHA-256:	039FE79B74E6D3D561E32D4AF570E6CA70DB6BB3718395BE2BF278B9E601279A
SHA-512:	C7B765B9AFBB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA878 041
Malicious:	false
Reputation:	high, very likely benign file
Preview:	GIF89a....w..!..MSOFFICE9.0.....sRGB......!..MSOFFICE9.0.....msOPMSOFFICE9.0Dn&P3.!..MSOFFICE9.0.....cmPPJCmp0712.........!......,...................'..;..b...RQ.xx.... ....,+..............................yy..;..b.........................qp.bb..........uv.ZZ.LL.......xw.jj.NN.A@....zz.mm.^_.........yw........yx.xw.RR.,*.++.. ....8....>......................4567...=..../0123.....<9:.()*+,-.B.@...."#$%&'....... !..... ....C.?....A;<...HT(..;

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Contract agreement.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 15:46:40 2022, mtime=Tue Mar 8 15:46:40 2022, atime=Sun May 28 20:16:55 2023, length=178975, window=hide
Category:	dropped
Size (bytes):	1059
Entropy (8bit):	4.56374243763475
Encrypted:	false
SSDEEP:	12:8M806jgXg/XAlCPCHaXZKBfB/YM+X+WTWwKQHu8juicvbE63D48QHu2NDtZ3Yil3:8m0/XTpKh2hBWfQlNeBQ7Dv3qo4yA7yJ
MD5:	9513D565031D67DBA8B2EBFE29BBA858
SHA1:	70DF1BD639F4907EB53012464120AE739D291AB6
SHA-256:	7A3760F8C3D3FC643BB0CA750770573A9F5F79EC27396394A916A7AB567E6306
SHA-512:	B1FD312F39DA121F7193B9E6A21D57487E651DDAD5610CF39DBD7C83B0B1495A359E9887D37278A3FEF2E7E0AE27972A6545C608696452EB889FE39E88055B6A
Malicious:	false
Preview:	L.................F.... ....P...3...P...3..'.................................P.O. .:i.....+00.../C:\..................t.1.....QK.X..Users.`.......:..QK.X*..................6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....hT...user.8......QK.XhT.*...&=....U..............A.l.b.u.s.....z.1.....hT...Desktop.d......QK.XhT.*..._=..............:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....x.2......V.. .CONTRA~1.DOC..\......hT.hT.*.../.....4..............C.o.n.t.r.a.c.t. .a.g.r.e.e.m.e.n.t...d.o.c.x......................-...8...[............?J......C:\Users\..#..................\\571345\Users.user\Desktop\Contract agreement.docx.......\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.n.t.r.a.c.t. .a.g.r.e.e.m.e.n.t...d.o.c.x.........:..,.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.......571345..........D_....3N.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Generic INItialization configuration [misc]
Category:	dropped
Size (bytes):	88
Entropy (8bit):	4.579734358584997
Encrypted:	false
SSDEEP:	3:bDuMJl+EUGjrjRUmxWt7GjrjRUv:bCYjrYCjrE
MD5:	554CBE79C94D699500455BDA9F6515D4
SHA1:	6A6E03D18EE83FB86C23BA306CC6D2D141B01912
SHA-256:	483C9CA9FBCD4BD95FBA5F6CB0415261D9D1C83D391B0C955C5AB5EAEBBD47CD
SHA-512:	7C7F871FE7DBB87D330B12F6174F129AB7E2A54AE51E7EA50B236AB8175D9660B1A060DFC1A7216C45688676E6130DA06CBA9F83224F623D551D67F7387C9DD
Malicious:	false
Preview:	[folders]..Templates.LNK=0..Contract agreement.LNK=0..[misc]..Contract agreement.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false

SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265 5
Malicious:	false
Preview:	.user..A.l.b.u.s.............p........15..............25.............@35..............35.....z.......p45.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Unicode text, UTF-16, little-endian text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~$ntract agreement.docx

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:	Microsoft Word 2007+
Entropy (8bit):	7.954541983842944
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	Contract agreement.docx
File size:	178975
MD5:	494ad369620d8b28dea9cc0d60b8f865
SHA1:	57c451f3c0af780141d663940d58c201cda2cf36
SHA256:	2390662435e396fea8f64f5d5cbf71f70e7c191b6568437a1b1f794846f316da
SHA512:	f91a2a536d161880aca47b18970aea6d795ff0c345cfa26401a936b9ecddf500100fbd0460b82fe5f75dbf4296e1cfdbb2c690bc07a0345c51009094c21ded82
SSDEEP:	3072:2lNuCUIljWXRhoC0Sf9bHpUHgl7Ms7EWyljC/o6fv5MTT3hegIHTulufd2o:2lrE9Z4gRMNW1/Q7hegIHTPd2o
TLSH:	080412EDE850EC17EAE34A758E44D6F5BBB8251282806DD367C0EF7C467094783069DE

File Content Preview:	PK..........!.6...............[Content_Types].xml ... (...

File Icon

Icon Hash:	65e6a3a3afb7bdbf

Network Behavior

⊘ **No network behavior found**

Statistics

⊘ **No statistics**

System Behavior

Analysis Process: WINWORD.EXE PID: **2188**, Parent PID: **576**

General

Target ID:	0
Start time:	14:16:56
Start date:	28/05/2023
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:	0x13f2c0000
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\Microsoft\Windows\Temporary Internet Files\Content.MSO\2BB8ABC6.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\93279D0F.jpeg	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\980DF3C4.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	6C7A0648	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$ntract agreement.docx	success or wait	1	6C7A0648	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2BB8ABC6.png	0	12033	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 04 1e 00 00 01 12 08 06 00 00 00 5a 5c 16 fd 00 00 00 01 73 52 47 42 00 fd fd 1c fd 00 00 00 04 67 41 4d 41 00 00 fd fd 0b fd 61 05 00 00 00 09 70 48 59 73 00 00 0e fd 00 00 0e fd 01 fd 6f fd 64 00 00 2e fd 49 44 41 54 78 5e fd fd 5f fd 65 fd 7d 1f 70 fd 49 fd 4c fd 58 51 70 22 67 70 12 70 6a 49 fd 06 13 42 fd 38 fd 50 1c 2c 3f 04 42 19 6b 04 21 21 0f 31 43 fd 1f fd 7d 71 21 63 3d fd fd 10 fd fd fd 60 6c 06 fd 50 6a fd 4e fd fd 10 02 79 fd 42 5c 08 fd 6e 1b 42 08 8c 2d fd fd 34 fd 38 4a fd 1d fd 56 6b fd 9d fd 57 5a 2b 3a fd fd 33 73 fd 39 7b fd fd fd fd fd fd 7d 46 73 75 fd 3e 6b fd fd 77 fd fd fd fd bc 79 fd fd 7b 00 00 00 00 1a 78 5d fd 13 00 00 00 60 70 fd 07 00 00 00 fd 19 fd 03	PNGIHDRZ\sRGBgAMA apHYsod.IDATx ^_e}pILXQp"gppjIB8P,? Bk!!1C}q!c=`IPjNyB\nB- 48JVkWZ+:3s9{}Fsu >kwy{x]`p	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\93279D0F.jpeg	0	16041	fd fd fd fd 00 10 4a 46 49 46 00 01 01 01 00 fd 00 fd 00 00 fd fd 00 43 00 02 01 01 02 01 01 02 02 02 02 02 02 02 02 03 05 03 03 03 03 03 06 04 04 03 05 07 06 07 07 07 06 07 07 08 09 0b 09 08 08 0a 08 07 07 0a 0d 0a 0a 0b 0c 0c 0c 0c 07 09 0e 0f 0d 0c 0e 0b 0c 0c 0c fd fd 00 43 01 02 02 02 03 03 03 06 03 03 06 0c 08 07 08 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c fd fd 00 11 08 00 fd 01 6f 03 01 22 00 02 11 01 03 11 01 fd fd 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b fd fd 00 fd 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 fd fd fd 08	JFIFCCo"}!1AQa"q2	success or wait	1	6C7A0648	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\980DF3C4.png	0	65536	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 18 00 00 00 fd 08 02 00 00 00 fd 0c 5c fd 00 00 00 01 73 52 47 42 00 fd fd 1c fd 00 00 00 04 67 41 4d 41 00 00 fd fd 0b fd 61 05 00 00 00 09 70 48 59 73 00 00 0e fd 00 00 0e fd 01 fd 6f fd 64 00 00 fd fd 49 44 41 54 78 5e fd fd 05 60 1c f5 3f fd d9 59 fd 5d 69 fd 2b 66 66 fd 2c fd fd 4c fd fd 26 69 fd 26 6d 86 fd fd 49 fd fd 49 1a 68 fd 40 03 4e fd 0e fd 72 65 4b fd fd fd 0c 2b fd fd fd fd fd 72 fd fd fd fd 7d 7f fd fd fd 0a fd fd fd fd fd fd fd 7b fd 3d fd 73 3e fd 9d 19 fd fd 79 fd 6f fd 13 61 fd 0f fd 0c 7d fd 1b fd 43 fd 07 35 fd 13 0b fd 71 0b fd 37 fd fd fd fd 3c 02 75 12 fd fd 46 fd 41 34 fd fd fd 2d 73 fd 99 69 fd fd 04 fd fd 7e 7c 6c fd fd fd 77 fd fd 24 3a 3a	PNGIHDR\sRGBgAMAapHYsodIDATx^`?Y]i+ff,Li&mIIh@NeK+r}{=s>yoa}C5q7<uFA4-si~|lw$::	success or wait	2	6C7A0648	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\Microsoft Office\Office14\PROOF\MSSP7EN.dub	unknown	4866	success or wait	1	7FEE914E8B7	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	1	success or wait	1	7FEE9140793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	4096	success or wait	1	7FEE91AAD58	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE9140793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE91AAD58	ReadFile
C:\Users\user\Desktop\Contract agreement.docx	155929	12033	success or wait	3	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2BB8ABC6.png	0	88	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2BB8ABC6.png	0	22	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\93279D0F.jpeg	0	88	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\93279D0F.jpeg	0	22	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\980DF3C4.png	0	88	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\980DF3C4.png	0	22	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\93279D0F.jpeg	0	16041	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2BB8ABC6.png	0	12033	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E287E699.png	0	44	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E287E699.png	0	44	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E287E699.png	0	44	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E287E699.png	0	44	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E287E699.png	0	1872	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E287E699.png	0	44	success or wait	1	6C7A0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E287E699.png	0	44	success or wait	1	6C7A0648	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6C7A0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6C7A0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6C7A0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\778A9	success or wait	1	6C7A0648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Wingdings	binary	05 00 00 00 00 00 00 00 00 00	success or wait	1	6C7A0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	6C7A0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	6C7A0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\778A9	778A9	binary	04 00 00 00 8C 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 31 BD E4 CD A9 91 D9 01 A9 78 07 00 A9 78 07 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C7A0648	unknown

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

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\P roducts\00004109D30 00000010000 0000F01FEC\Usage	ProductFiles	dword	1455161400	1455161401	success or wait	1	6C7A0648	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\P roducts\00004109D30 00000010000 0000F01FEC\Usage	ProductFiles	dword	1455161401	1455161402	success or wait	1	6C7A0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resili ency\DocumentRecovery\778A9	778A9	binary	04 00 00 00 8C 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 31 BD E4 CD A9 91 D9 01 A9 78 07 00 A9 78 07 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 8C 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A9 78 07 00 A9 78 07 00 00 00 00 00	success or wait	1	6C7A0648	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

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

Disassembly

⊘ **No disassembly**