

JOeSandbox Cloud BASIC



ID: 682720

Sample Name:

suddenlinkfile08.11.2022.doc

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 21:39:57

Date: 11/08/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report suddenlinkfile08.11.2022.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\92EA7B6A.png	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D2BD0FCD.png	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{85143033-14FB-4D6C-A896-4B71FF6886D1}.tmp	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6BA42A8C-94A7-4B9D-AE9D-169FEB5183D7}.tmp	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B4FFB3A4-1FA7-4CB0-A4A7-82E371C5BC92}.tmp	11
C:\Users\user\AppData\Local\Temp\~DF701D4A450A56331E.TMP	11
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	11
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\suddenlinkfile08.11.2022.LNK	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\~\$ddenlinkfile08.11.2022.doc	13
Static File Info	13
General	13
File Icon	13
Static OLE Info	13
General	13
OLE File "/opt/package/joesandbox/database/analysis/682720/sample/suddenlinkfile08.11.2022.doc"	13
Indicators	13
Streams with VBA	14
VBA File Name: ThisDocument.cls, Stream Size: 2811	14
General	14
VBA Code	14
Streams	14
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 369	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: 5100	14
General	15
Stream Path: VBA/_SRP_3, File Type: data, Stream Size: 2724	15
General	15
Stream Path: VBA/dir, File Type: data, Stream Size: 486	15
General	15
Network Behavior	15
TCP Packets	15

Statistics	15
System Behavior	16
Analysis Process: WINWORD.EXEPID: 2644, 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

suddenlinkfile08.11.2022.doc

Overview

General Information

Sample Name:	suddenlinkfile08.11.2022.doc
Analysis ID:	682720
MD5:	3b6a5f7e4f048cb..
SHA1:	a2f68a276e0b18..
SHA256:	e9258541a5c96f..
Tags:	doc IcedID
Infos:	

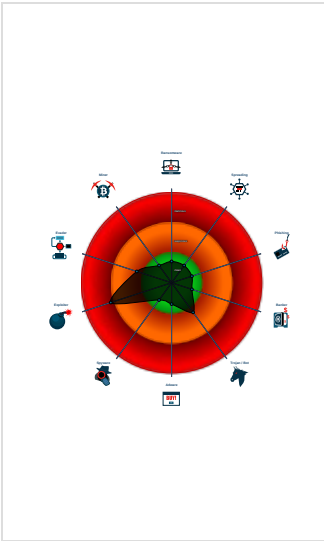
Detection

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: 2644 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



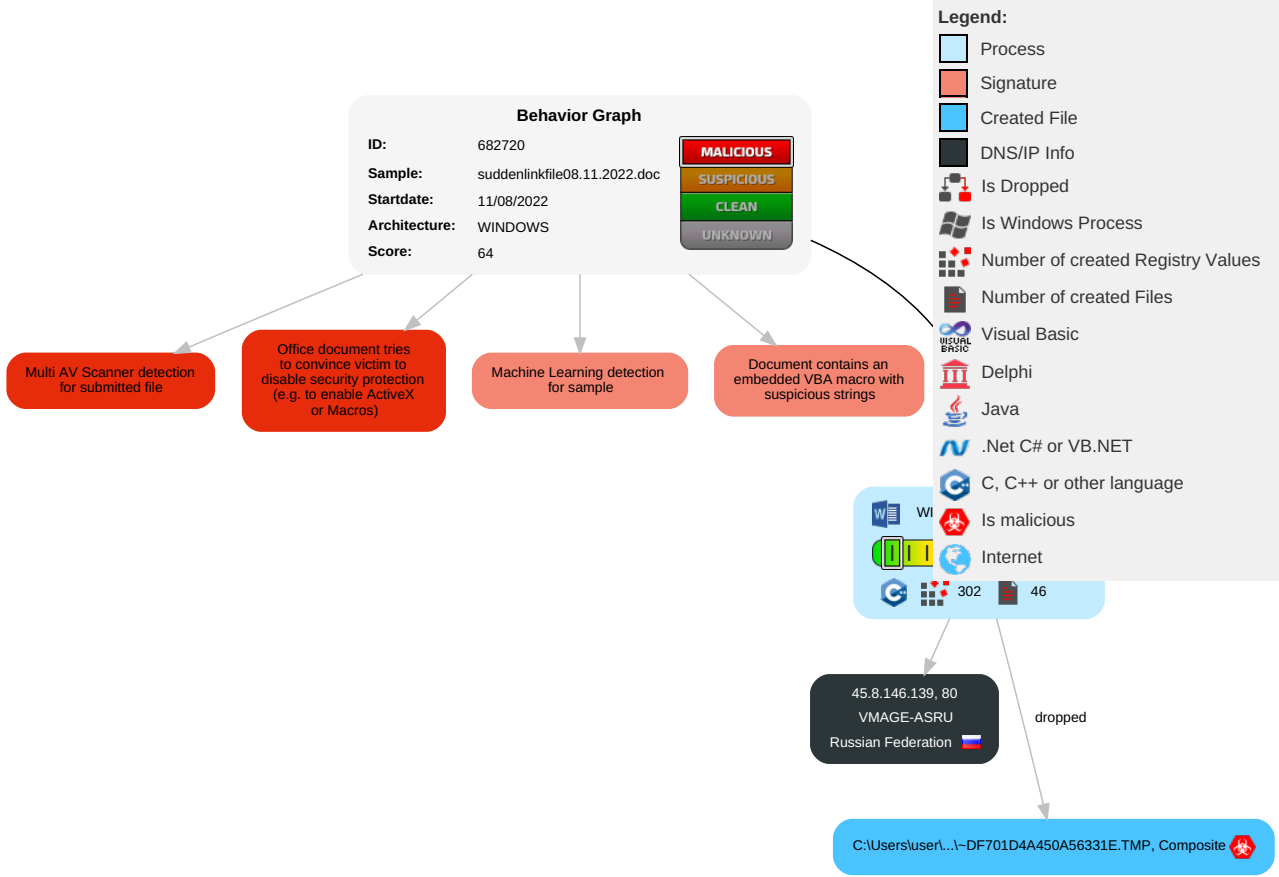
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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	<div>12</div> Scripting	Path Interception	Path Interception	<div>1</div> Masquerading	OS Credential Dumping	<div>1</div> File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	<div>1</div> Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	<div>1</div> Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	<div>1</div> Disable or Modify Tools	LSASS Memory	<div>1</div> 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)	<div>12</div> 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

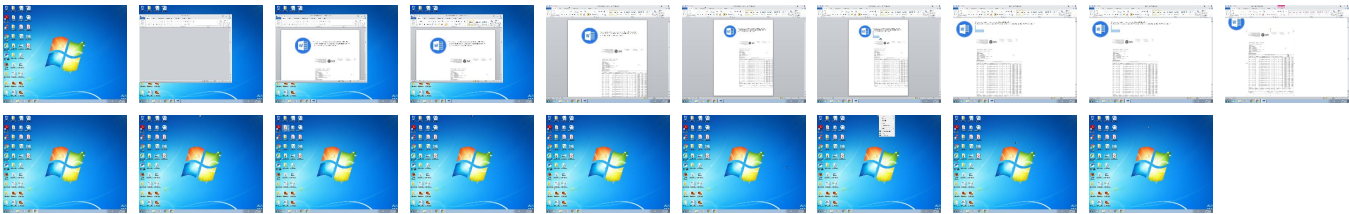
Behavior Graph

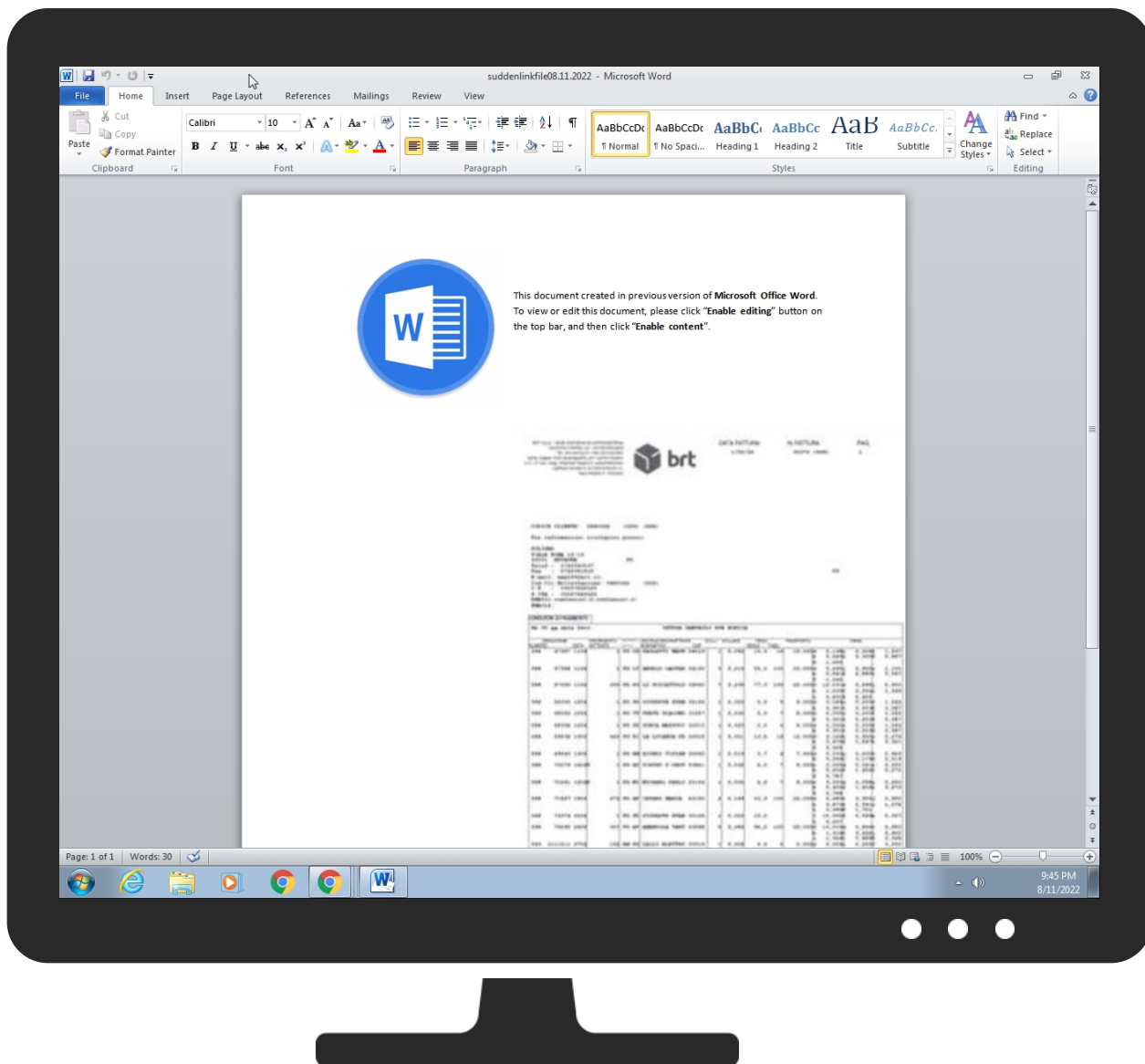


Screenshots

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
suddenlinkfile08.11.2022.doc	26%	Virustotal		Browse
suddenlinkfile08.11.2022.doc	18%	ReversingLabs	Script-Macro.Trojan.Amp hitryon	
suddenlinkfile08.11.2022.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF701D4A450A56331E.TMP	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

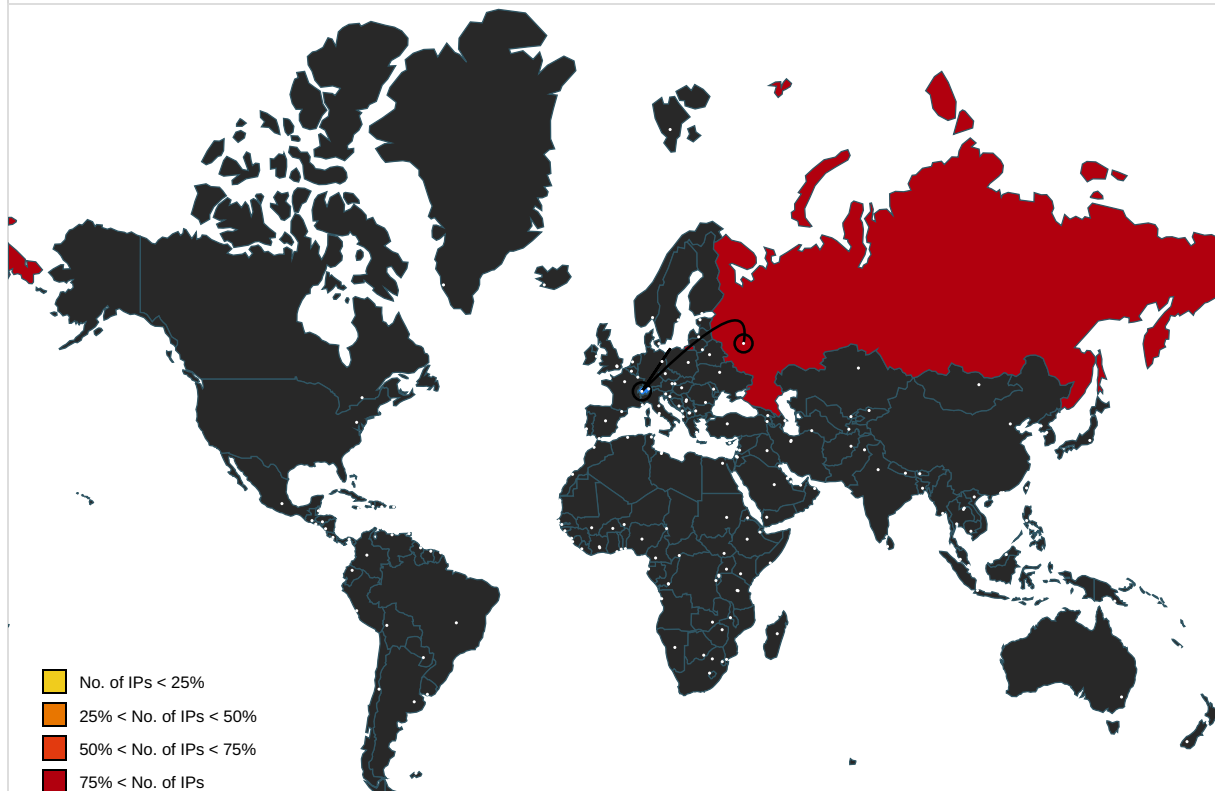
⛔ No Antivirus matches

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:	682720
Start date and time:	2022-08-11 21:39:57 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	suddenlinkfile08.11.2022.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Run name:	Without Instrumentation
Number of analysed new started processes analysed:	4
Number of new started drivers analysed:	0
Number of existing processes analysed:	0


Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	<ul style="list-style-type: none"> • HCA enabled • EGA enabled • HDC enabled • 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\92EA7B6A.png 	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 404 x 560, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	129793
Entropy (8bit):	7.991103599335203
Encrypted:	true
SSDEEP:	1536:U4MtqqxENTB01ei3aAl/AKK/7zwFACKTMFIUSYEoa8aFSK0fLeCmRSqr4Ho0FK7T:vMIKWtY3ligvSiaYRLmQliHMIzTKI
MD5:	AF92425A49BAE0E026E6ED210EAD4FD2
SHA1:	1BE112AF7400BF91B305597286E3BA5BA54C8D2D
SHA-256:	2745C121B3DF782FDA4D684B264ED6BEC8303B3C85F695A268D633BB9756DAE0
SHA-512:	09638DB753DA0A3FF748217578EDD72F270917406F9786C14564C7A822B43D93084BA22B3E5EFA8523D6DB912CB4A1E0E84E0002D157AFC65A9B5D5B9B5E486:
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....0......IDATx...s...H...Q.%_L235US.r...x^.....[...l.y.Y_... K.T.J.H.....u...^o3.x.1%...?g.)._...X.....s.. ...lk...{{^..8N.....4.<{wEY..2.x.1...c2}..y...^e.o...3.dv~....wgX.. _.....T*.V...^.....{.....y...+.n.f&3^..y..g.....yf...x..y...m.....x>.1&.L..3..z..3..x...e.JzKfL.x...v~G..M..{>.....?x}..<v....Q...7Y.}...uYm..6g.j.....}...^..S..._g..r.....IP...q....7_x.C...b.%7_V...>..m~..<...=.s.m.v.../..jyY..~4..O6....3q....+u...x.v.=M...s...Z....}y..d..*9b...=...x..4...G.&dY...o...+M...l.gYV*..\$).J.R.wy...)./.....N.^{...s....."K^")...P..n...E_y1.g.....p....)/(^.jg..h.Fk.b_...<{.l....._?./...?J.(.H.I.E.b.n....v.<{O...}@... ..<.;w.zvo..?y... xt!...R.jt...Rv~.7.Oy..G.j.r..".?8E.P.....B.T...y;.....U...!.....h.U.si..[w.]x.x..4M..\.'ze.-Fl.....5.).@...}.2mD;.....l.;..n..2.u..".g..g\$.6...`0_..M.uU6[.w.;]..



C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D2BD0FCD.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):	256096
Entropy (8bit):	7.979290280978911
Encrypted:	false
SSDEEP:	6144:M3Y5ZrfMaWvOqQjH5OHjYDoadLgGB7AgFMg9bdY5aD:MoLfmX8YjY3gk9bdSaD
MD5:	2B87DAB37C0E64FC69EF97114CD433AE
SHA1:	4277610AF912B13E6C5F79C1787E17512D3CB662
SHA-256:	11ED29EF2888F5D9F52BE4BB54EC2A3BAD6A6DA8CBC6A986ABFB960590D2AE30
SHA-512:	B1B9695E19A783B5A967884E72683412B819BA0E5CD48D9728601F83EF7164E8A7115AE509616B131AEDC1C5EF5792D4EB6AE575B2F031A107CF890DAE66E476
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs..!...!.....IDATx^...fGU..*3.W...z?...^?..l.....8....'.Al.Q.HBB..@.B:=%...@.4.!F...0...L.).1.0&)...k....i...Z.j.....}.5..M..?.w.H...i...=zO_.....1)!Tz+{.1...r.).;..k9..k.)Qu.....< .?.U..6.g... E...nl...,G#...O\$o.LEO?.mH...r=..F...tVyB...Z'y)..E.g..3..J...r..E.2c..WZ;&5..").f.i.U...Q...-...5..X.ce...^..z...k. ...m\...W~.....qK...2..1^..-.....n.^..=K.Z...D..5..L.ZZ.0...z2.6K...r.....f.*{/...z...]. ..A.k.....mh.U.n.^..z.r.R..i+.r.1.t"...^..l.....-...A...D...h.m.....up@O...S...=...1z....L'Z.0&.H.2-.qK\$.D.oQ.m."e{.N...^5.*...0h.....C.*f.2.l.z.v.T\$.[Z....]*?.^C.+.....=,...N>Qy5.%Sy=.L+[!..Md:...].V.....Pe...8..8...l..H^3.j;QeZ.{f{.Z.U..h.f.le2.6.....2..S.3\$.+....*...n\..O.3.j.E.7&.l.q..^.%dkhq8.Z>...l.....[z.U...L"i5.r5..3.....ek..+. ...*j.....T^..g..Z..*7.2..6...o.g...-;...Z...7.@.YtB...*.zR.X

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{85143033-14FB-4D6C-A896-4B71FF6886D1}.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):	28672
Entropy (8bit):	4.012537878999086
Encrypted:	false
SSDEEP:	384:nht157EVVu7wmf1NFXkz51PtKp7EVVu7wmf1NFXkz51:n057EHjyOYP7EHjyO
MD5:	12671CC9F739236F9775BAD3D752F2A0
SHA1:	A69DAC909354B36545F77264988E83F436415163
SHA-256:	4B6B4A548ED6EEEDDF2217673D056E200868CBF0AAF6D55F01A90CD04CBB938D
SHA-512:	4DFE0E1E45B8A6B32D52A5207B8D2BAC4E746D7A1ACDA1E40E26845574AC6373F87E485C759FAA4C16E3166F1A6E2C0DE1ACF8569DFF84E0AC11404D1DBFC149
Malicious:	false
Reputation:	low
Preview:>.....(.....4..).....*...+...../..0..1...2..3...5..6.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6BA42A8C-94A7-4B9D-AE9D-169FEB5183D7}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.1363686128594344
Encrypted:	false
SSDEEP:	12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82l+akwkvFpG41g48e4PlI5EHkUZl8/W4c:4LG1ND9Pxn82UakZGkg4YMHjJz
MD5:	6EF3EA8101C8504360DA98C4874E7C42
SHA1:	047D0D54A1CEBB77EA382B6325071BFB68662CD1
SHA-256:	A1C41EBCD1AF5BEC8D46C575A6CA571C63F1B882A1F80DD227D7AE10A8B08F88
SHA-512:	0941D92448D238CF49FA2AAFD81563F46AF2520D842E492BBA024A7A48FD7B5EC4B4765595179C0FDDDBFE2B2CF86BB9B721788816D431542EA6151301B63FC1
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{B4FFB3A4-1FA7-4CB0-A4A7-82E371C5BC92}.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\~DF701D4A450A56331E.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):	4.158343579575897
Encrypted:	false
SSDEEP:	768:Kj8ynkngoPlp2cVdXo/txRbQ+o7EHjpIP6WZGvZd7ka3GFao9ITK:KYjngAlpxdXo/txRM2q6eGL7HGFaT
MD5:	066010C2883634E03243536E71C971F2
SHA1:	84163B8F0E2F6BE40A4F9BC2B9B6E6D410F20F5B
SHA-256:	5BD9A14DD5B018366EE04FD6A4DF0C541F17164DD2894F2E8068B292D6357D43
SHA-512:	9DC4D55B0325D043847C70AA4125D7BC503FC88BB73543DEFE82E0EF5CA99932D1E6F4FB306EA0FB5D2DAFDB8B093B8D3BFC5903B138A50CDBBB174ABBD AEE25
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.....h...U...V...W...X...Y...]...[...\......i..._.....a..b..c..d..e..f..g..Z.....j...k..t..m..n...o..p..q..r..s...^.....

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):	99
Entropy (8bit):	4.644735439919192
Encrypted:	false
SSDEEP:	3:bDuMJIOUBA9MLs!Yj9omX1Xw9MLs!Yj9ov:bC6oK7Yj9OK7Yj9y
MD5:	6EF1C4B749DFF30D0B3C286D1DC65F3D
SHA1:	DBA1564C758F374CC424B56A0B94EFEF9207A926
SHA-256:	96616B6B94968109EC8B6F850C90192ACD4D4E7D943F3CAEC152268B0C69736
SHA-512:	BB554EC4558B05FB85F82E5AE1EC51B4BF1D3D5A2126A19581B9F53873BA159446D60010D3ECBB95132909E204D8891518414BD1F5C069A97C0744975005D420
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..suddenlinkfile08.11.2022.LNK=0..[doc]..suddenlinkfile08.11.2022.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\suddenlinkfile08.11.2022.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 03:44:12 2022, length= 2366716, window=hide
Category:	dropped
Size (bytes):	1084
Entropy (8bit):	4.5419912135321105
Encrypted:	false
SSDEEP:	12:8V0REC60gXg/XAICPCHaXBKBnB/eLX+W2CaigYicvb5vsj9Pn2DtZ3YilMMEpxR2:8euq/XTRKJMYCtaey9+Dv3qfu7D
MD5:	F961E5AC176027EC869B9C42B8B2ABF9
SHA1:	39DFB2F53B3A0FDD7A0F69165038266E29147071
SHA-256:	EF109B54F64772043F5962A1A0949D1ECB11D3D226F677F5790126F12F622EB9
SHA-512:	1371EBCCCEA72239626EE96C4EE97F77A11610B22406A61E989EC460CA352F4B9BC7F7370011B5CDF64D0CFBD32D0B4B11FDABBE458C633E57DE8EEEE98AE4DA4
Malicious:	false
Preview:	L.....F.....X#..3..X#..3@+.....\$.....P.O.+00../C:\.....t1....QK.X..Users.`.....:QK.X*.....6....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-2.1.8.1.3.....L.1.....hT.....user.8.....QK.XhT.*...&=....U.....A.l.b.u.s.....z.1.....hT....Desktop.d.....QK.XhT.*..._.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-2.1.7.6.9.....2...\$.U.%..SUDDEN~1.DOC..f.....hT..hT.*..r.....'.s.u.d.d.e.n.l.i.n.k.f.i.l.e.0.8...1.1...2.0.2.2...d.o.c.....-8...[.....?J.....C:\Users\.#.....\305090\Users.user\Desktop\suddenlinkfile08.11.2022.doc.3.....\.....\.....\.....\D.e.s.k.t.o.p.\s.u.d.d.e.n.l.i.n.k.f.i.l.e.0.8...1.1...2.0.2.2...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\Templates\~\$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJyIp2bG/WWNJbifGUiD/n:vdsCkWtz8Oz2q/rViXdH/I
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E572676CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728DC608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDF4533BC9E428B0637562AFA
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB

SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~\$ddenlinkfile08.11.2022.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJyIp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/I
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AFA
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

Static File Info	
General	
File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993948464282991
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:	suddenlinkfile08.11.2022.doc
File size:	2366716
MD5:	3b6a5f7e4f048cb005496243fe2a019e
SHA1:	a2f68a276e0b18cb1f11745d9046f4ffa1b1a428
SHA256:	e9258541a5c96fcacb6a2ce349282db7e9403a16fa9f952e8f1f69929dda7abc
SHA512:	f8e777ebbf8ef85d0299552f8580adf97af8eb236fd94f998c47417369bebbfeb54882ca34dcd60c9444cc4624fa0f8d8f32c8037abe29dd50a0b6f478c842f1
SSDEEP:	49152:~YswLHjvPXNnVtQ8364b8ulhZ3fR4Bit3soDB1Nu8aSSaz:~HyDv/hVtQ8K449hZvOit3sU1NWZu
TLSH:	5FB533BF108D46C7E51892FD24DE357412EA8AF18A32FC02A85D851A14A17FF96E7F31
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/682720/sample/suddenlinkfile08.11.2022.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: 2811

General

Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2811
Data ASCII:	.B.Attribute VB_Name = "ThisDocument"...BasicNormal...VGlobal!.Spac.IfA.Ise.JCrea.tabl. .Pre decla.Id..#Tru."Expose..TemplateDeri.v.\$CustomlizC.P....D.? PtrSa.fe Function Lib "us.er32" Alias "Set.Timer" (ByVal... .. As Long.9, ...
Data Raw:	01 42 b4 0d 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: 369

General

Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	369
Entropy:	5.3102107547738004
Base64 Encoded:	True
Data ASCII:	ID="{62DA6FD2-8ADE-45CC-8D66-6236941671A8}"..Document=ThisDocument/&H00000000..Name="Project"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="C6C42C6834E8FEECFEEECFEEECFEEEC"..DPB="8C8E66BEEA85EB85EB85"..GC="5250B8FC7FFD7FFD80"....[Host Extender Inf
Data Raw:	49 44 3d 2d 7b 36 32 44 41 36 46 44 32 2d 38 41 44 45 2d 34 35 43 43 2d 38 44 36 36 2d 36 32 33 36 39 34 31 36 37 31 41 38 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 d0 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:	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: 5100

System Behavior

Analysis Process: WINWORD.EXE PID: 2644, Parent PID: 576

General

Target ID:	0
Start time:	21:44:13
Start date:	11/08/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13fda0000
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	6E092B14	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\--DF701D4A450A56331E.TMP	success or wait	1	6E110648	unknown
C:\Users\user\Desktop\~\$ddenlinkfile08.11.2022.doc	success or wait	1	6E110648	unknown

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

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

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	6E001925	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	6E001925	unknown
C:\Users\user\Desktop\suddenlinkfile08.11.2022.doc	1964413	185	success or wait	2	6E110648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D2BD0FCD.png	0	65536	success or wait	4	6E110648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\92EA7B6A.png	0	65536	success or wait	2	6E110648	unknown

Registry Activities

Key Created


Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E0EA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E0EA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E0EA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E110648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E110648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E110648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\78D90	success or wait	1	6E110648	unknown

Key Value Created	
1. Customer Satisfaction	Increased customer satisfaction scores by 15% through personalized product recommendations and responsive customer support.
2. Operational Efficiency	Streamlined internal processes, resulting in a 20% reduction in operational costs and a 10% increase in productivity.
3. Market Expansion	Successfully entered new markets, increasing the company's reach and generating an additional 30% in revenue.
4. Employee Engagement	Implemented a comprehensive employee training program, leading to a 25% increase in employee engagement and retention.
5. Brand Reputation	Enhanced the company's brand reputation through strategic marketing campaigns and positive social media interactions.

[illegible]

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400100000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784306	1426784307	success or wait	1	6E001925	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	6E001925	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	6E001925	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	6E001925	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	6E001925	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	6E001925	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	6E001925	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\78D90	78D90	binary	04 00 00 00 54 0A 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 2D 9B 70 5A 06 AE D8 01 90 8D 07 00 90 8D 07 00 00 00 00 00 DB 04 00	04 00 00 00 54 0A 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 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 90 8D 07 00 90 8D 07 00 00 00 00 00 DB 04 00 00 00 00 00	success or wait	1	6E110648	unknown

Disassembly

 No disassembly