Joe Sandbox Cloud BASIC

ID: 682722
Sample Name:
suddenlink.doc.08.11.22.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:35:28
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2

Windows Analysis Report suddenlink.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\BBC84C8E.png 10
  - C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D18A7737.png 10
  - C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{7D800B62-4169-49B4-82C2-03F10C50B5DB}.tmp
  - C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{55E0F33F-3C33-4FD8-B916- 10
    02BB3F3865BE}.tmp 10
  - C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E11EF5ED-C44F-4253-A2FB-74DC7A3642DF}.tmp 11
  - C:\Users\user\AppData\Local\Temp\~DFAD7C0BB457B0CC55.TMP 11
  - C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat 11
  - C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\suddenlink.doc.08.11.22.LNK 12
  - C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm 12
  - C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex 12
  - C:\Users\user\Desktop\~$ddenlink.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/682722/sample/suddenlink.doc.08.11.22.doc" 13
      - Indicators 13
    - Streams with VBA 14
      - VBA File Name: ThisDocument.cls, Stream Size: 2764 14
      - General 14
        - VBA Code 14
    - Streams 14
      - Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 357 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

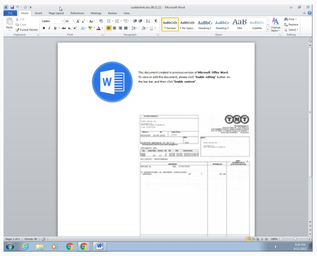
Statistics 15
System Behavior 16
Analysis Process: WINWORD.EXEPID: 2972, Parent PID: 576 16
General 16
File Activities 16
File Created 16
File Deleted 16
File Read 16
Registry Activities 16
Key Created 16
Key Value Created 17
Key Value Modified 18
Disassembly 22

Windows Analysis Report

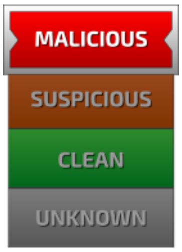
suddenlink.doc.08.11.22.doc

Overview

General Information

Sample Name:	suddenlink.doc.08.11.22.doc
Analysis ID:	682722
MD5:	13f0a9bd5a2a4fd.
SHA1:	bb6d3ab2c01d30..
SHA256:	04042893124fdb..
Tags:	doc IcedID
Infos:	
	

Detection

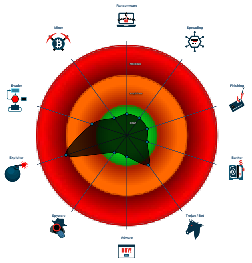


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 2972 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

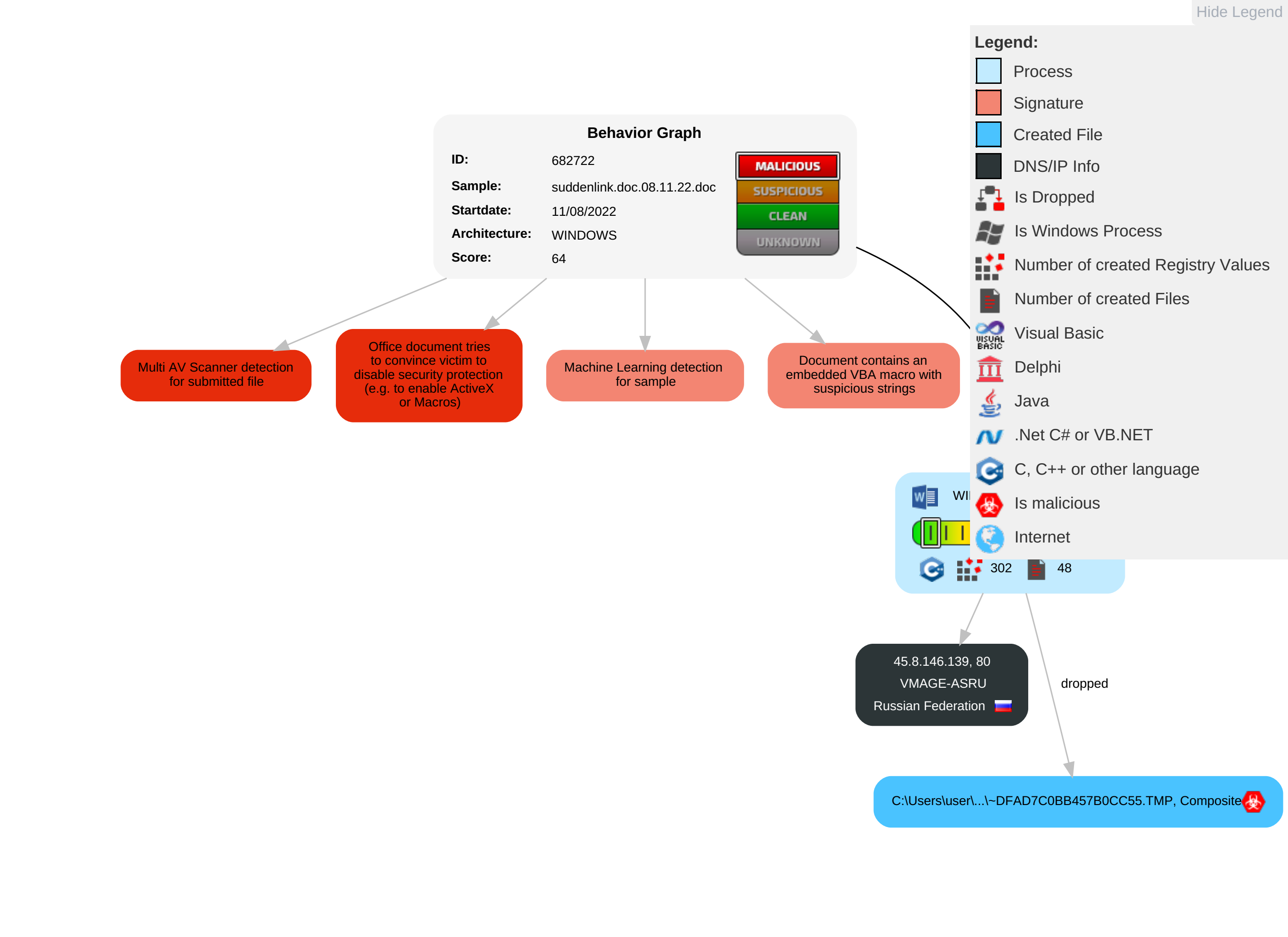
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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



Behavior Graph

ID: 682722

Sample: suddenlink.doc.08.11.22.doc

Startdate: 11/08/2022

Architecture: WINDOWS

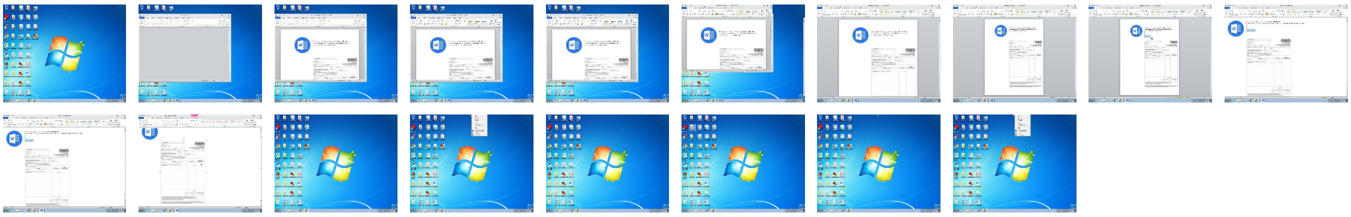
Score: 64

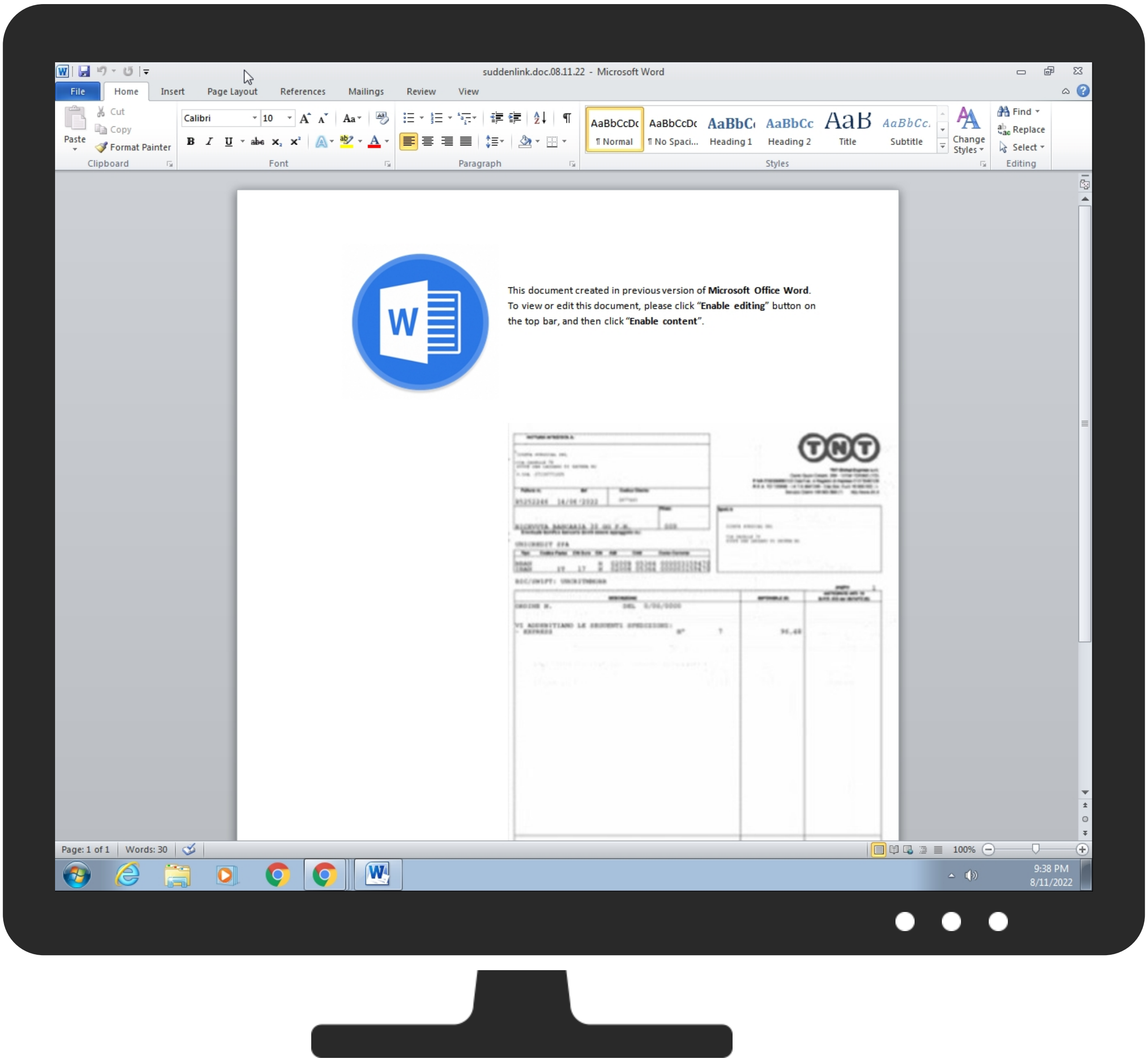
Hide Legend
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Multi AV Scanner detection for submitted file
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
Machine Learning detection for sample
Document contains an embedded VBA macro with suspicious strings
WI
302
48
45.8.146.139, 80
VMAGE-ASRU
Russian Federation
dropped
C:\Users\user\...\~DFAD7C0BB457B0CC55.TMP, Composite

Screenshots

Thumbnails

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





This document created in previous version of **Microsoft Office Word**. To view or edit this document, please click "**Enable editing**" button on the top bar, and then click "**Enable content**".

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
suddenlink.doc.08.11.22.doc	18%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
suddenlink.doc.08.11.22.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DFAD7C0BB457B0CC55.TMP	100%	Joe Sandbox ML		

Unpacked PE Files

⊘ **No Antivirus matches**

Domains

⊘ **No Antivirus matches**

URLs

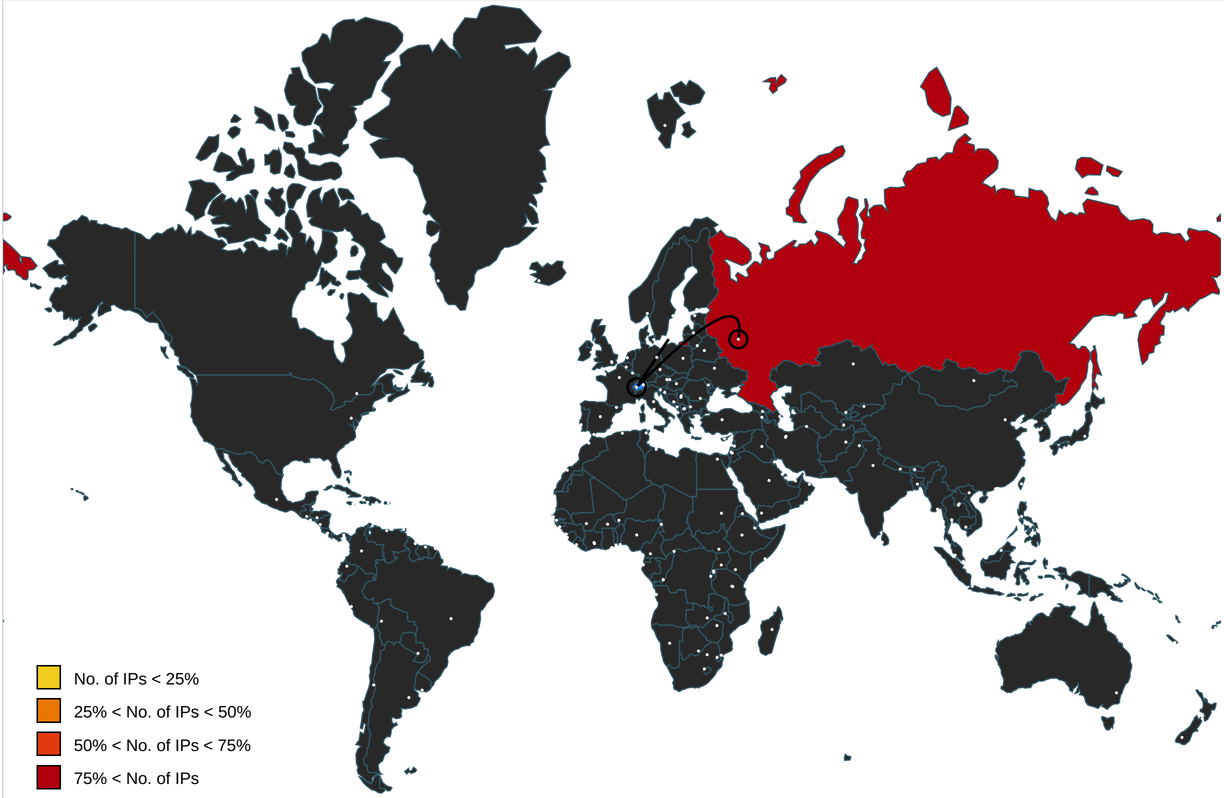
⊘ **No Antivirus matches**

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:	682722
Start date and time:	2022-08-11 21:35:28 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	suddenlink.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:	- 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:	- Successful, ratio: 100% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	- 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, t oo many NtQueryAttributesFile calls found.
- VT rate limit hit for: suddenlink.doc.08.11.22.doc

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\BBC84C8E.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):	256025
Entropy (8bit):	7.98021203163416
Encrypted:	false
SSDEEP:	6144:x+Js5bWmwngQ8+C5K7jGQvBxyLuv/YQ2M2xkUfpaj:xcstWmIrC54qGxyKozMW/pq
MD5:	A510821080102B59B41A4B4F7517A2E9
SHA1:	0DE77D02B1EC5854FB491938966A1F21A45B6342
SHA-256:	C00890A5BD755B16A7EDD3639B0499D2DF25D47C1B7869D66DCFDCF4C1128655
SHA-512:	5A993B2FAF68F531EA18473952ECE1E208668789D4652647A8D8B1DD98CB219F6A367AF746FAB3AB73E16DB5AC85EAD3FAB2F24B3408B103445DC47C3886F76 A
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR.............7......sRGB.........gAMA......a.....pHYs..!...!..........IDATx^....fWU.3#*m.C......G..$.H$(.B..Q@R.3.@T..!!..2.......J.@...$Dh.j....L........1u...}..U;.<....>.k...k........k..K\C..=1F..>C....2...aL>.&..!...P.}!.4...k.V.H...LM'.\..,......<..dH........kG..C..2..J#$2.r.c.I....z.h...d[^...0k.3n....5...Yc...y..AO.H.../......z+."uW.......i..Z~"...[...zj.j.Z(.u.Z.*WQ.*?..W...k........E..k....#..Z^b..T~..6M......O....t.^C../.5ni..+w.h.I...5....4....h.GB.|^..'].5T....lE...L{..^....d..d..[.^..g.5_i=T..L.1.....|.@MW@o.A+..4....f.-=Q.K...a..........r....E[~V.m.d..Ue2nQef...+..1...7A..k.h.=~.J.eA.+..'.\..Vn...=]....m.X..C+.\.Y<Pym...1.P...2I'T.SCE.-...A....^....|;....JT.5.Z^.U..yP....t.z....{r....LW~"iU...4h. iI...f.. dG..)W.g..r-..=.^iI..k.+...6..g..k.H..\.Z..y..[..L....C.k...o.5..h.......Np...P..d.....iO.|..v.A.......X....t..zr5..K.U.\.^..{@...#.?&..m..o.u|.c.5_.....|...W..A.+..V........m...z<@:....Z..,.q.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D18A7737.png

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 380 x 526, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	79862
Entropy (8bit):	7.9850226558494
Encrypted:	false
SSDEEP:	1536:3oqyPqib6IbiXmcfDBFdEU8yslk2ZGBlGUCk4+:3yqtImXmcbBFopLwlGDkH
MD5:	F673388F14A0B0E6160D7E31FB8B27A7
SHA1:	792480CA5B43D57E2A0A65466D77A294DA9D55C3
SHA-256:	0D79507FBC5D3C1843F0584E92FFD8B8F2862B4AE569BEB934963B30185E6489
SHA-512:	957C95FE8ED7DC213F027C59952F3F2AB5DFE6ED91944880D230AFC7B2B9EFFD812000FBF26CD6948DD3C478CB9B049C97405F6EBD4A86E3D10241DA3A0B69 2A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG........IHDR...|.........4.!... .IDATx...{#...9g...p...l.+....^x..[..'.....9...g.K.t7.0#...Ca....S..[o.:.N:.v.'......r...W...q.....!......q.CF.g..._.c.y........,;9....6.._z...,./.....nt.../..g.t..._......._./.-......F......+mt.X.../...+...0:......./.^.{...b.}.`0.X,....V..|.8N0.$..\...@0....l.ZqB.+?_...fR}....%.\.....Y,.\|A..r..Z..B~8..t.P.~.Cc[p.D.W.INn...f....5....c.If.V....Oh$Y...|....GI......q... .....u.../....b.`.0.L.@ 0.L..@(.......Ac..Rd...o...........6~x..v..t.._...Ph6.E"...... .T.._,..p..e.1.o......qf.uk/.km/w.Z..<...9.'.|>..B.PH.....K.J.8...$.;.\|>g...A..3\..'._e....pX6x..(..m....Kc6...a.By;.P..R..M.u..p2.\|....7..0V.kO..n...v#..\|>.....pm.....B..$..-..h4:.N#..r..D"|n<...ak..`0.k.g....d@q..Cf<wk..oW.....5.....V.U.+$.*...?.2..r..6...}:=.e.j.I.)/....*....Y..t:.L.......vG.H...t.j....:..`0..FL.H$....d.P(..DB...j%.....g.Y..<??o.Z...t.....l.P(.r.X,&k..._.Fm>..Z....^.7...)...8.X.X,...t:..Dd-.{%......y.8.x<...h6..H$.H.\..`;[..O....(.....B

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{7D800B62-4169-49B4-82C2-03F10C50B5DB}.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):	5.7631575162306445
Encrypted:	false
SSDEEP:	192:bDtmZ1e4NVASSur6+vpanaB7tmZTe4NVASSur6+vpaJaB:3tu9OJW6+vpdts9OJW6+vp
MD5:	072FB75C3A4BF5B517705352E4E67615
SHA1:	627A92E9E10586A5E126BF05120520C323915F2B
SHA-256:	822CC2E3C2F9575E88C466BEEF7D7CF7F17A21E1C5793FF9D545796F3793090D
SHA-512:	0443747823284504439CBA7513B624FBFB12AC6D643AB86881A4E178F939921682E3EB432544E007FD65B8D4763854095C61C119ED2720C1CB46D6FFC3BBCEC2
Malicious:	false
Reputation:	low
Preview:	.....................>..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{55E0F33F-3C33-4FD8-B916-02BB3F3865BE}.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:DMlzfRLZRW4WZ1MFKuQ9cc3xn82lshakwkvu4i454PllYHkUZR+/W4c:4LG1ND9Pxn82Shak4fCY+H/rz
MD5:	74E435B7E86AE8D08CA309653AC019E8
SHA1:	1D3153EDA5F56D7CD7EB4425BD484D4A8F3FB1BC
SHA-256:	ADBA871414A54C8C7B84F54CCBE7CAD9BA87CECB3BEF81C21CA4C780A8B73F31
SHA-512:	F72B908A7533B2EC9A2CFB5036F1BF44DA2C3509BFD9F0EDA0C3ACEF711C045AC10163F8605BBF928891E9F2B80068FD125DA5C0A828351C2F6F7A000BB6613 9
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{E11EF5ED-C44F-4253-A2FB-74DC7A3642DF}.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\~DFAD7C0BB457B0CC55.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):	4.171149550824995
Encrypted:	false
SSDEEP:	1536:8bbjTBY5IAOJfuRNpB9UR+8GGmu/jycAGfah:8fjTB0IJluRNpA+8GGnjycAGfa
MD5:	991BAB333ED521918DA66C5C45EB8223
SHA1:	274D1EE5B5D4B1C324562227EFFCD6B6B6333C1D
SHA-256:	98F773985361A8F3CB1F388560760A769BBEE23A30C4AD3018886AD90F620A96
SHA-512:	A021D005346A818496937E753AE90AD939C4CC7FF6BE74B0CA16B4F4AE6166F45B8A2E8CF820FACEDD1960289E15F56F0E48CE544C16211BC370213370BD758
Malicious:	**true**
Antivirus:	• 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\index.dat

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

File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	97
Entropy (8bit):	4.617781427614191
Encrypted:	false
SSDEEP:	3:bDuMJlOUBA9ML0dRjbUmX1Xw9ML0dRjbUv:bC6oK0dlbCK0dlb2
MD5:	135F37C6E324A5EBBB0F7836C0183C93
SHA1:	72FC8344F3415FCB1D989CCB08EBD69706883E79
SHA-256:	DE33429FABCDA46B35EED5271B897FF22DCD3E666FBFC203052B0DD094EC8449
SHA-512:	81E0519BA192D1BB2BCE5ABEDE7CFEC424886051CB0F2E0ED994027DC58644AFAC8DA33E284FC283E2A3E9E81048FC9B182ED86FFF15B13C38E98209477E96 91
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..suddenlink.doc.08.11.22.LNK=0..[doc]..suddenlink.doc.08.11.22.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\suddenlink.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 15:45:53 2022, mtime=Tue Mar 8 15:45:53 2022, atime=Fri Aug 12 03:37:11 2022, length=2221142, window=hide
Category:	dropped
Size (bytes):	1079
Entropy (8bit):	4.534102984705601
Encrypted:	false
SSDEEP:	12:87VCpU0gXg/XAlCPCHaXRBktB/eLX+W9E/xgign4Cicvbc/v0dldannqDtZ3Yilc:87cek/XThOMHE/xflJeQkdl1Dv3qIu7D
MD5:	0109BB67A2799D7B42508A9C1CDD2580
SHA1:	8595E889ED21D7D530EC788DD5154E70050C6C57
SHA-256:	04E847822A1F68CAAA5259DA1AA7F3CD1DD769F4F62C6A82E1634BC9E6B636E8
SHA-512:	68F799092C645CC23A9E60CE303BC6861BB2F4CC2296BEFC48206B0F7DDD4285BA05E42D2553124FC95A77F59C778B4C0719A1266898F3AA7872C489E842777
Malicious:	false
Reputation:	low
Preview:	L.................F.... ....!...3...!...3....(0....V.!.........................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.V.!..U.$ .SUDDEN~1.DOC..d......hT..hT..*...r.....'..............s.u.d.d.e.n.l.i.n.k...d.o.c...0.8...1.1...2.2...d.o.c.....................-...8...[............?J......C:\Users\..#...................\\936905\Users.user\Desktop\suddenlink.doc.08.11.22.doc.2.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.s.u.d.d.e.n.l.i.n.k...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.......93690

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
Malicious:	false
Reputation:	moderate, very likely benign file
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\~$ddenlink.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:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AEA
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):	7.993530464050495
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:	suddenlink.doc.08.11.22.doc
File size:	2315700
MD5:	13f0a9bd5a2a4fd90924a953eb9b1642
SHA1:	bb6d3ab2c01d3058964cd6493a691ad9971307ca
SHA256:	04042893124fdbf007cfdb673ef878ac9a47f37f871c1e5322ec46945915abc1
SHA512:	4a5d5d80a802886231ff33a37f2bb5e319aee424fe965e69638e77491680543885514bd314e633e2be51475b5585705b0ed1d111bc4dd612d94e82f7a725fc9b
SSDEEP:	49152:T/6jUrhhEP6jf4bkgrMk3tuXBJzExnppCcssLxoO:TyjTijf8IFxJzqppCEoO
TLSH:	49B533C47306AF5D811748F0201FBF87EA705485A71B935929ABF68DCEF260DB2C794A
File Content Preview:	PK..........!..U~............._rels/.rels...J.@............4.E..D.....$....T..w-..j........|.zs..z..z.*X.%(v......6O.{Pl........`S__._x .C..CR....:....t..R......hI.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/682722/sample/suddenlink.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: 2764

General

Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2764
Data ASCII:	..Attribut.e VB_Nam.e = "Thi.sDocumen.t"...Bas..1Normal...VGlobal!.Spac.lFa.lse.JCrea.tabl..Pre decla..Id..#Tru."Exp.ose..Temp.lateDeri.v.$CustomlizC.P.... .D.? PtrSa.fe Funct ion .....Lib ".user32" .Alias "K.illTimer." (ByVal.. As Long.', ...#.&....).#P"
Data Raw:	01 bf 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: 357

General

Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	357
Entropy:	5.311948833105888
Base64 Encoded:	True
Data ASCII:	ID="{AB2E814C-A2DF-4438-9993-4F276A344AE0}"..Document=ThisDocument/&H00000000..Name="Project"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="383AE71DEB1DEB1DEB1DEB"..DPB="7072AF50B050B050"..GC="A8AA778878887877"....[Host Extender Info]..&H000000
Data Raw:	49 44 3d 22 7b 41 42 32 45 38 31 34 43 2d 41 32 44 46 2d 34 34 33 38 2d 39 39 39 33 2d 34 46 32 37 36 41 33 34 34 41 45 30 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 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:	1.9253220393231318
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . 8 . . . . P . . . . " . . . . q . . . . A . . . . ` . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . `) . . . .
Data Raw:	72 55 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 11 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 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 00 a1 07 00 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:	2.6961948881008246
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . x . . . . . P . . . . p . . . . ` . ! . . . . . . . . . . . , . . p . . . . . . a . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . ` . a . . . . X . . p . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 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 00 00 00 00 78 00 00 00 08 00 50 00 b1 08 00 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 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:	6.299718761930016
Base64 Encoded:	True
Data ASCII:	. . . . 0 . . . . . . H . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . * W d - . . . " . < . . . . r s t d o . l e > . . s . t . . d . o . l . e . (. . h . . ^ . 9 \\ G . { 0 0 0 2 0 4 3 l 0 - . . . . C . . . . 4 . 6 } # 2 . 0 # 0 . # C : \\ W i n d . o w s \\ s y s t e m 3 2 \\ . e 2 . . t l b # O L E . A u t o m a t i . o n . E N o r m . a l E N C r . m . a F . . c E V C . . . . (m . ! O . f f i c g O . f Q . i . c g . . g 2 D F 8 D 0 4 . C - 5 B
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 2a 57 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 01 39 5c 47 00 7b 30 30 30 32

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 21:36:21.845629930 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 21:36:24.844556093 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 21:36:30.913180113 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 21:36:42.927454948 CEST	49172	80	192.168.2.22	45.8.146.139
Aug 11, 2022 21:36:45.921857119 CEST	49172	80	192.168.2.22	45.8.146.139
Aug 11, 2022 21:36:51.928256989 CEST	49172	80	192.168.2.22	45.8.146.139

Statistics

⊘ **No statistics**

System Behavior

Analysis Process: WINWORD.EXE PID: **2972**, Parent PID: **576**

General

Target ID:	0
Start time:	21:37:12
Start date:	11/08/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13ff00000
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	6E1F2B14	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DFAD7C0BB457B0CC55.TMP	success or wait	1	6E270648	unknown
C:\Users\user\Desktop\~$ddenlink.doc.08.11.22.doc	success or wait	1	6E270648	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	6E161925	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	6E161925	unknown
C:\Users\user\Desktop\suddenlink.doc.08.11.22.doc	1871619	184	success or wait	2	6E270648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BBC84C8E.png	0	65536	success or wait	4	6E270648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D18A7737.png	0	65536	success or wait	2	6E270648	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E24A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E24A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E24A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E270648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E270648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E270648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\787A6	success or wait	1	6E270648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\787A6	787A6	binary	04 00 00 00 9C 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 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 50 80 11 5F 05 AE D8 01 A6 87 07 00 A6 87 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6E270648	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 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	6E161925	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	6E161925	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	6E161925	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	6E161925	unknown
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	6E161925	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	1426784306	1426784307	success or wait	1	6E161925	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	6E161925	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	6E161925	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	6E161925	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	6E161925	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	6E161925	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	6E161925	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\787A6	787A6	binary	04 00 00 00 9C 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 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 50 80 11 5F 05 AE D8 01 A6 87 07 00 A6 87 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	04 00 00 00 9C 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 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 A6 87 07 00 A6 87 07 00 00 00 00 00 DB 04 00 00 00 00 00	success or wait	1	6E270648	unknown

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

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 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 FF FF FF FF				

Disassembly

⊘ **No disassembly**