**ID:** 682773
**Sample Name:** [name removed]
file 08.11.2022.doc
**Cookbook:**
defaultwindowsofficecookbook.jbs
**Time:** 00:19:09
**Date:** 12/08/2022
**Version:** 35.0.0 Citrine

# Table of Contents

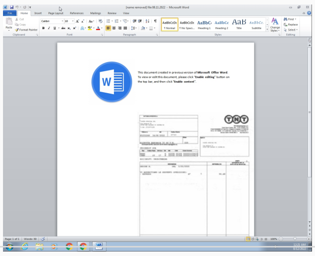
# Windows Analysis Report

## [name removed] file 08.11.2022.doc

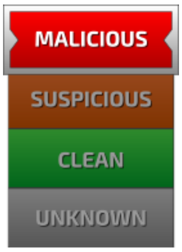
## Overview

### General Information

| | |
|---|---|
| Sample Name: | [name removed] file 08.11.2022.doc |
| Analysis ID: | 682773 |
| MD5: | 4f487d329bcf514.. |
| SHA1: | 52d9885233394a. |
| SHA256: | d66a64e64a1d1b. |
| Tags: | Bokbot<br>doc<br>IcedID<br>macros<br>MonsterLibra<br>Shathak<br>TA551 |
| Infos: | |



### Detection

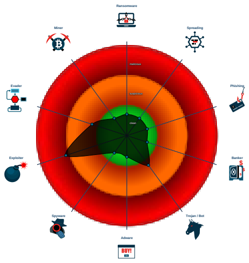


| | |
|---|---|
| Score: | 64 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### 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: 1056 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

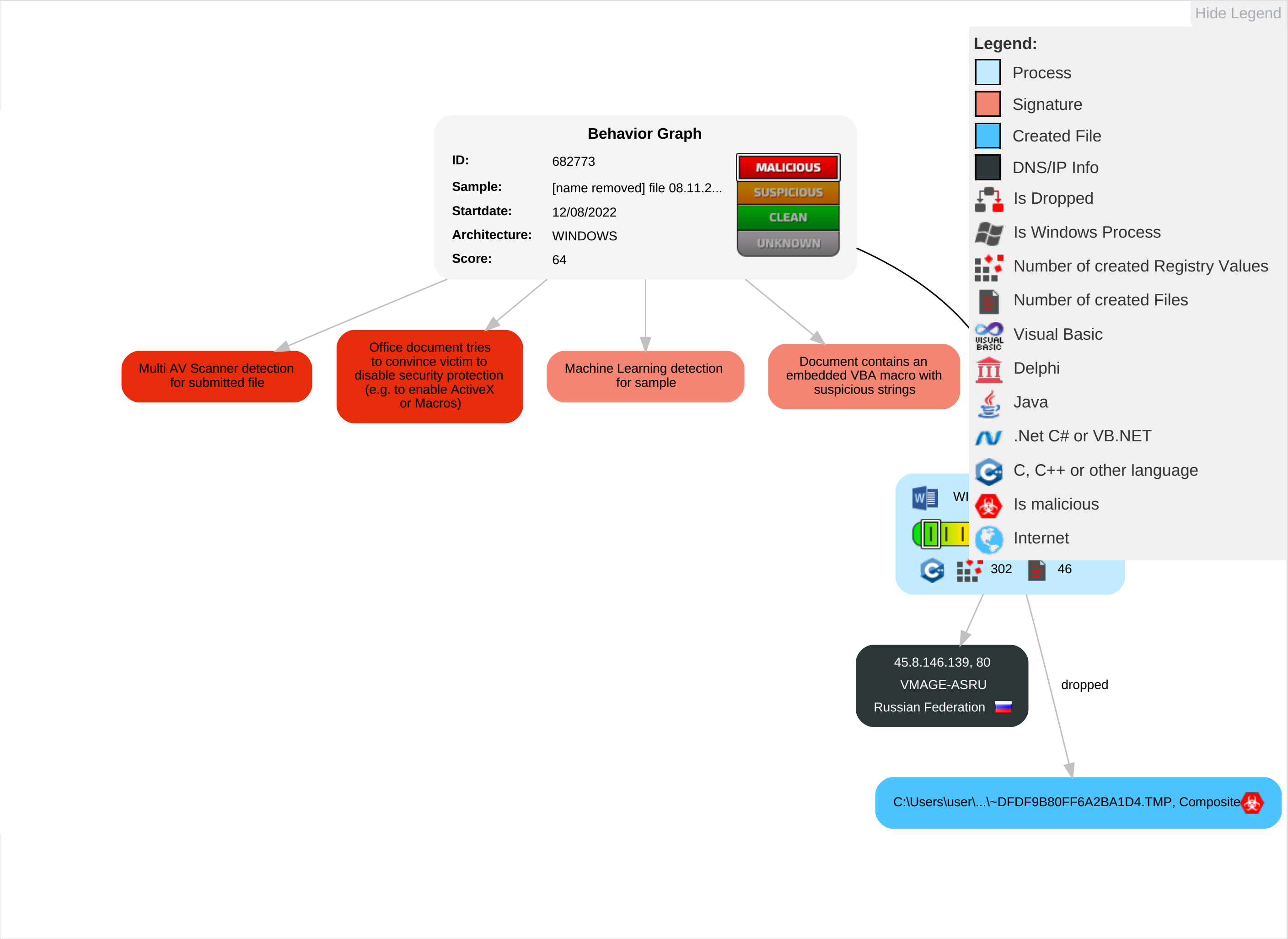
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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<br>Scripting | Path Interception | Path Interception | 1<br>Masquerading | OS Credential Dumping | 1<br>File and Directory Discovery | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | 1<br>Ingress Tool Transfer | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |
| Default Accounts | 1<br>Exploitation for Client Execution | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | 1<br>Disable or Modify Tools | LSASS Memory | 1<br>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<br>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: 682773

Sample: [name removed] file 08.11.2...

Startdate: 12/08/2022

Architecture: WINDOWS

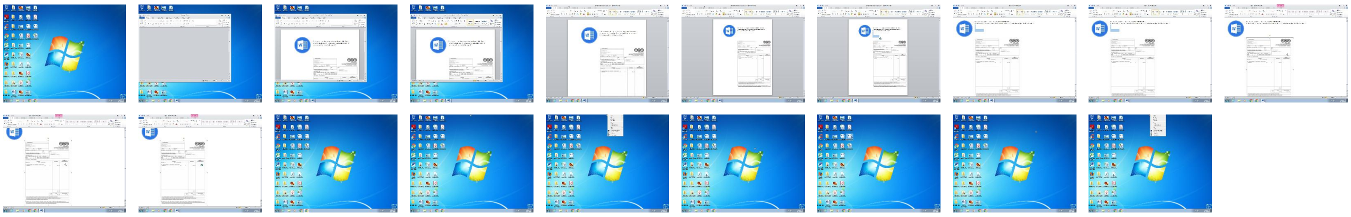
Score: 64

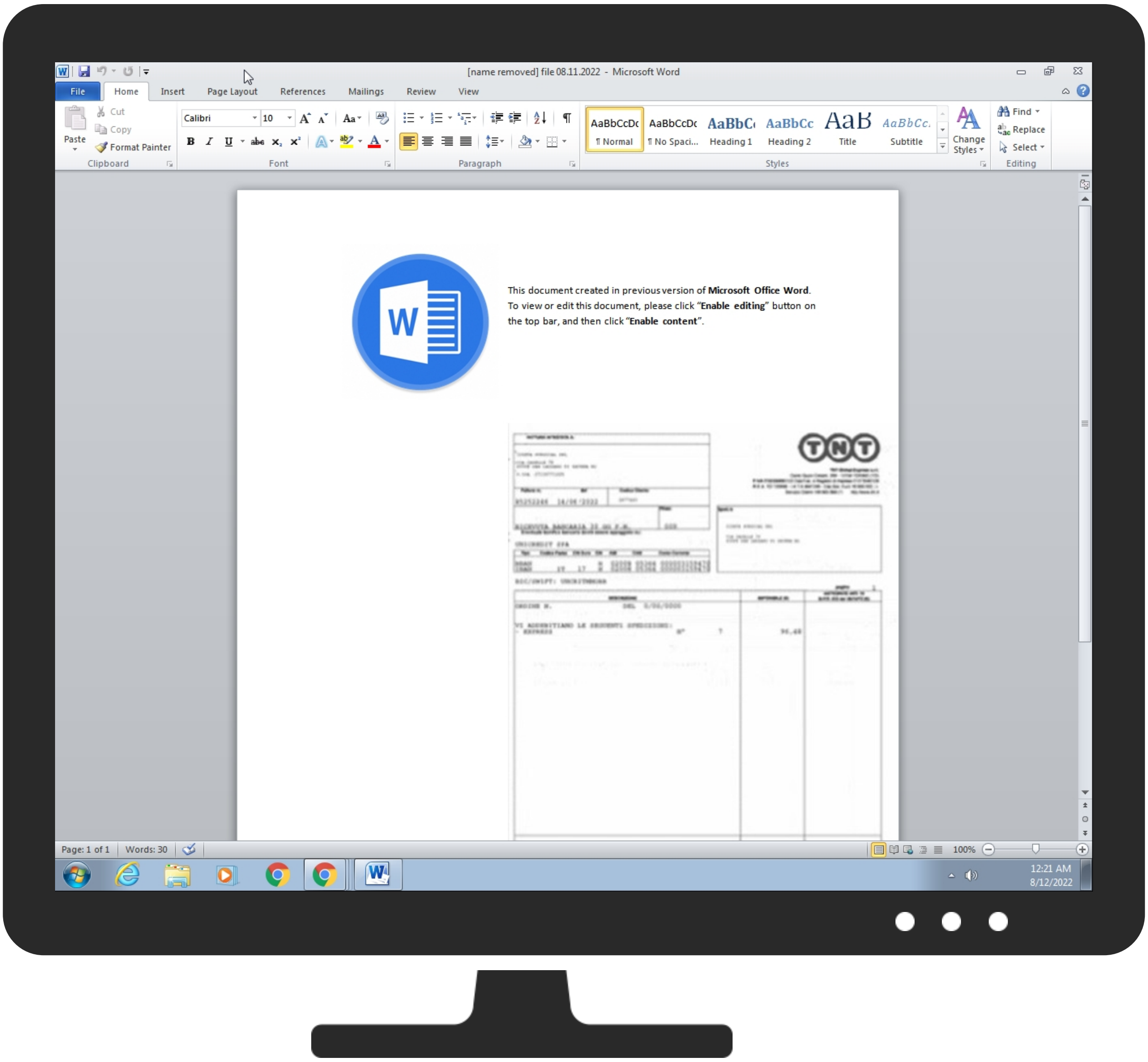
Hide Legend
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Multi AV Scanner detection 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
46
45.8.146.139, 80
VMAGE-ASRU
Russian Federation
dropped
C:\Users\user\...\~DFDF9B80FF6A2BA1D4.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 |
|---|---|---|---|---|
| [name removed] file 08.11.2022.doc | 27% | Virustotal | | Browse |
| [name removed] file 08.11.2022.doc | 20% | ReversingLabs | Script-Macro.Trojan.Amphitryon | |
| [name removed] file 08.11.2022.doc | 100% | Joe Sandbox ML | | |

### Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\~DFDF9B80FF6A2BA1D4.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

🟨 No. of IPs < 25%
🟧 25% < No. of IPs < 50%
🟧 50% < No. of IPs < 75%
🟥 75% < No. of 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: | 682773 |
| Start date and time: | 2022-08-12 00:19:09 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 5m 10s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | [name removed] file 08.11.2022.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) |
| 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<br>• EGA enabled<br>• HDC enabled<br>• GSI enabled (VBA)<br>• 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%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Found application associated with file extension: .doc<br>• Adjust boot time<br>• Enable AMSI<br>• Found Word or Excel or PowerPoint or XPS Viewer<br>• Attach to Office via COM<br>• Scroll down<br>• 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\2197A182.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): | 256215 |
| Entropy (8bit): | 7.978353630345434 |
| Encrypted: | false |
| SSDEEP: | 6144:eAJt7vvFhw7UBHzZiKVixZs+63Jby+hvEaAWirPosx4gR:eAzDfhH1nVWh63J9mbxnR |
| MD5: | C46CBD511D9669284EA364D93575B594 |
| SHA1: | 3754D9E8FE6F6D2B9946215D7EAB1F27AFCF55DE |
| SHA-256: | C79BCF4CCCFCAC32F26C892F6196BE3D299CEAA4DC157E633F73E470534B9F90 |
| SHA-512: | 2D3FE353D3D3DBBF5671DD780E4B2ADD4E62F32291091CDBD3757DE3F2665A69A99CDD6987368DE1271A14BA3432B853D4A1B55226B07CABDB06AF31D4A30 A3 |
| Malicious: | false |
| Reputation: | low |
| Preview: | .PNG........IHDR.............7......sRGB.........gAMA......a.....pHYs..!...!..........IDATx^....fGU..3.W...}......*$.a..1... .)aT.(*...h......tw..!.!.  F....p..Q&....s.O.I..>........Ju..4..'.U..U..VU. s...9.-.~.!..+.R.8..2.S..2=..U..j[.g>..<....@....l..q.W....m..h.UO..+....,.q.c......+.....r-f.....=z..J.t...f]....n....'*..{.c.:@/.PQ.....A....6.C.I=..R.mo.W9.....OT.,....c1h.-5M..VT...2.q.. .to\Lk.k.E..6]c.........lE-..g.....*..z..Zz...e@/.qMg.R..'..m\..UZ..]..P.1Z.[..T...^..k.._..'.h.W...=...*2..U.m.6].5n...\|.Y..=.7.WT..zeg......h.\|.r..he.B".m\Qy=>H^....=z..0....5..>.....J.t..- .t$2.:2O..@.'z40K...5..r.o......k....ek.him...I....2...*..'...Z.^>C..+...%P.X..o....K.1 .a.=.^.3........3.Bo<.m[..6.Z~.h..+.....w...>..+.[$o.L..9>I.U..,..6.P.y_.l-...^N4Hz.e....+-.he..-Z... .....\|.L......lz.z.4.. ...g\...Lb.\|E.S....ZT~O6i..'.\..\|K.q".9.....V...gHTZ..h.J.hice.W..^?k.D...2...h.=.l_.....*V..W.6]...'.l.\........mj..D+.........^.0&.i.^uW~...k......%.J...2. |

### C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E4BEFF9B.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: | 957C95FE8ED7DC213F027C59952F3F2AB5DFE6ED91944880D230AFC7B2B9EFFD812000FBF26CD6948DD3C478CB9B049C97405F6EBD4A86E3D10241DA3A0B6 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{8452E96F-6729-4A2C-AB1E-1C2D1EF9A762}.tmp

| | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | Composite Document File V2 Document, Cannot read section info |
| Category: | dropped |
| Size (bytes): | 12288 |
| Entropy (8bit): | 5.677809127217584 |
| Encrypted: | false |
| SSDEEP: | 192:/dKtAce49Xx64Zb1ayJaOtuhe49Xx64Zb1ayJa:YtNDx601HDtuDx601H |
| MD5: | 8827DC93D63651073FF3D011B57BF666 |
| SHA1: | 2BD8699CCD852F86830E1D73679DF57993155D37 |
| SHA-256: | 07641445DE45DE90065330B760C9B3C3D1A3473546E662143D6DBCF43D5E3D28 |
| SHA-512: | F67892A95D25D925FC6CD5322BF992887B12D50E2A98DBB4767E9AB867CC07129958109FB2EF60A4C92CF298CB15ECEC97D2EBAC44A6083072D9B384630428 C |
| Malicious: | false |
| Reputation: | low |
| Preview: | ......................>.................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................. |

### C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{D18A3924-35A8-4945-B934-02C37A6660AC}.tmp

| | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1536 |
| Entropy (8bit): | 2.1334198335541092 |
| Encrypted: | false |
| SSDEEP: | 12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82l2kwkvOqe44ee4Fe4PllQeHkUZx/W4c:4LG1ND9Pxn820kQyeKeYueHKz |
| MD5: | 58591290AE843606AF0D6B57469A64EF |
| SHA1: | C3E627CD8D44DF24D3B43BF0728705872B2D021C |
| SHA-256: | BB1DA4F35C31DEC55F874526BCC7BF941BE529C1543A6AD93B606F52542D7BEF |
| SHA-512: | 25103E9352EA576E1C9BE49741A62FB8FB777598FB4AF8CDC823A3C0E1EE440A7F36A57D39301692EAE2335614BC30ABD8A7E162A80C99D0C37C3A1D244FED5 |
| 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{E87DA6BC-D94B-493D-9994-A22FC53CFF23}.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: | 95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4 |
| Malicious: | false |
| Reputation: | high, very likely benign file |
| Preview: | ................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................... |

### C:\Users\user\AppData\Local\Temp\~DFDF9B80FF6A2BA1D4.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): | 60928 |
| Entropy (8bit): | 4.161709890278296 |
| Encrypted: | false |
| SSDEEP: | 768:imxbVW7ydujuVk1T3JRdXh3gfYE3glEbDJWgGvPF5rOKztGPaF:1+7NjuVk17rdXh3gAWBGF5y8tGPaF |
| MD5: | 0AA0A325FBEB7B84A87A7AE24066BD06 |
| SHA1: | 04ED0BD033D6072EE60C8F8832D4F45032D42568 |
| SHA-256: | 907D19C07FBC33DAFEBD196406829D3A28D758F1DF7FEBD3E4D050FCB297E988 |
| SHA-512: | 45E165FF14C423C4008F017E00B06310030C8D46AFBF09339716D840951BA904121E7FC8DB15AD6148BA3099371D50E2F224F8EC62A56928062731E09E47405C |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Joe Sandbox ML, Detection: 100% |
| Reputation: | low |
| Preview: | ......................>.........................................................................................................................................................................................................................................................................................................................................................T...........(................................................................................................................ ...!..."...#...$...%...&...'.......)...*...+...,...-......./...0...1...2...3...4...5...6...7...8...9...:.......<...=...>...?...@...I...B...C...D...E...F...G...H...;...J...K...L...M...N...O...P...Q...R...S.......i...V...W...X...Y...Z...^...\...].......j...`.......b...c...d...e...f...g...h...[.......k...l...u...n...o...p...q...r...s...t..._...................... |

### C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\[name removed] file 08.11.2022.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 15:45:51 2022, mtime=Tue Mar  8 15:45:51 2022, atime=Fri Aug 12 06:20:09 2022, length=2221308, window=hide |
| Category: | dropped |
| Size (bytes): | 1114 |
| Entropy (8bit): | 4.5846487299704375 |
| Encrypted: | false |
| SSDEEP: | 12:8bsM/Eu0gXg/XAlCPCHaXWBlXB/zxkpX+WeRWihNicvbnp9Ne3DtZ3YilMMEpxRn:8oL/XTm3xqIRph0et9M3Dv3q2u7D |
| MD5: | FC813F79C155DA267AC957C0A13F8923 |
| SHA1: | 58E5F7F1EECFE36AC7AC74FEB3CD850D7944DE7A |
| SHA-256: | 41B7417DFF2400AECA44D39935DAED9BA1852FDCA4D365ECBC542071600F2D4A |
| SHA-512: | C6DDA4D36B2BB2A42D97A2F7CB6DB50867D9DEEB5F60AD4C35E0687F25A9E5C2918D0AC4D389A54058C3116F5F35ECFC3E5AAD3ECA5CD09D6209A9C0E193<br>DD18 |
| Malicious: | false |
| Reputation: | low |
| Preview: | L.................F.... ....q...3...q...3...U'.......!.........................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...!..U.: ._NAMER~1.DOC..r......hT..hT..*...r.....'..............[.n.a.m.e. .r.e.m.o.v.e.d.]. .f.i.l.e. .0.8...1.1...2.0.2.2...d.o.c......................-...8...[............?J......C:\Users\..#..................\\581804\Users.user\Desktop\[name removed] file 08.11.2022.doc.9.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.[.n.a.m.e. .r.e.m.o.v.e.d.]. .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. |

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

| | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 111 |
| Entropy (8bit): | 4.681898743278708 |
| Encrypted: | false |
| SSDEEP: | 3:bDuMJlmZMY9omX10EIDMY9ov:bC/p9stp9y |
| MD5: | 9BC76A86E561F0AD5CCCC2B07508F10A |
| SHA1: | A3A8922B60793BC5016BEFB8F64F66C0EFF3E9E3 |
| SHA-256: | 05A0762C3D99AE2CB2ACDC936A53CF2B33F963E3F114BEF75DA728AE68F5E91C |
| SHA-512: | B7EBDCAA5085B9723A4A340DE4C805C3034DDD07C73CC9678D774737AF16800A07CD152AEAE049D4294D733BBD12D9E72F1FBD4608E3302BB9E06B13EDB60<br>DA |
| Malicious: | false |
| Reputation: | low |
| Preview: | [folders]..Templates.LNK=0..[name removed] file 08.11.2022.LNK=0..[doc]..[name removed] file 08.11.2022.LNK=0.. |

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

| | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 162 |
| Entropy (8bit): | 2.503835550707525 |
| Encrypted: | false |
| SSDEEP: | 3:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l |
| MD5: | 7CFA404FD881AF8DF49EA584FE153C61 |
| SHA1: | 32D9BF92626B77999E5E44780BF24130F3D23D66 |
| SHA-256: | 248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7 |
| SHA-512: | F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE<br>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: | 98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D<br>4 |
| Malicious: | false |
| Preview: | .. |

### C:\Users\user\Desktop\~$ame removed] file 08.11.2022.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:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l |
| MD5: | 7CFA404FD881AF8DF49EA584FE153C61 |
| SHA1: | 32D9BF92626B77999E5E44780BF24130F3D23D66 |
| SHA-256: | 248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7 |
| SHA-512: | F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE<br>A |
| 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): | 7.993668516736907 |
| TrID: | • Word Microsoft Office Open XML Format document (49504/1) 49.01%<br>• Word Microsoft Office Open XML Format document (43504/1) 43.07%<br>• ZIP compressed archive (8000/1) 7.92% |
| File name: | [name removed] file 08.11.2022.doc |
| File size: | 2316250 |
| MD5: | 4f487d329bcf514575a0c8e5a4dcb53f |
| SHA1: | 52d9885233394acffdda1ea3a40989a8b47e9e34 |
| SHA256: | d66a64e64a1d1b44ebcc854f04b1e175ccc93b61fff0f093394f6dcdcd785d82 |
| SHA512: | 2fbe8609658dc2caa3a9e74227b69e1fd52fb86482794881d4f61cb635536f961f78b93cf73d4d387c8717e10d1232aa6ceac68c0d7a7f8de190743ebf832b1e |
| SSDEEP: | 49152:TnxBpMvUTIyOgNz8bc10IsulzqMy44elEAU33SapcOnaT54Z1+bBOz:TxBpMavFNzUcuIsul+d44e1y3VIV4rY2 |
| TLSH: | 36B533B0C86EBA19CA01AD3389D3546E35ABD427FB3D5C478053890B76DB558FEE2881 |
| File Content Preview: | PK..........!..U~............._rels/.rels...J.@............4.E..D.....$....T..w-..j........\|.zs..z..z.*X.%(v......6O.{Pl........`S__._x .C..CR....:....t..R......hl.3..H.Q..*.;..=..y... n.......yo.......<br>[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/682773/sample/[name removed] file 08.11.2022.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: 2846

### General

| | |
|---|---|
| Stream Path: | VBA/ThisDocument |
| VBA File Name: | ThisDocument.cls |
| Stream Size: | 2846 |
| Data ASCII: | .n.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 ".KillTime.r" (ByVaxl ........ As Long,, ....../... |
| Data Raw: | 01 6e 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: 369

#### General

| | |
|---|---|
| Stream Path: | PROJECT |
| File Type: | ASCII text, with CRLF line terminators |
| Stream Size: | 369 |
| Entropy: | 5.262779644813546 |
| Base64 Encoded: | True |
| Data ASCII: | ID="{B35AB5D0-15B8-4F33-8DA0-8EDBCA2B4B0A}"..Document=ThisDocument/&H00000000..Name="Project"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="8587941D9CA6A0A6A0A6A0A6A0"..DPB="0A081B9CA19DA19DA1"..GC="8F8D9E1BA6252A262A26D5"....[Host Extender Inf |
| Data Raw: | 49 44 3d 22 7b 42 33 35 41 42 35 44 30 2d 31 35 42 38 2d 34 46 33 33 2d 38 44 41 30 2d 38 45 44 42 43 41 32 42 34 42 30 41 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 . . . |

| General | |
|---|---|
| Data Raw: | cc 61 ff ff 00 00 00 |

### Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 5116

| General | |
|---|---|
| Stream Path: | VBA/__SRP_2 |
| File Type: | data |
| Stream Size: | 5116 |
| Entropy: | 1.9231245259582155 |
| Base64 Encoded: | False |
| Data ASCII: | rU@...............@.......@..............8..............................P..........."...............q.......... .............................A..............`...........................................`)"....................... ................ |
| Data Raw: | 72 55 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 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 03 00 50 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 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: | 2.6915430960066646 |
| Base64 Encoded: | False |
| Data ASCII: | rU@...............@.......@.......................................x.....P..............p................1....... ...........`.1............,..p......q..................................a.........................`............X..p..... ................... |
| Data Raw: | 72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 |

### Stream Path: VBA/dir, File Type: data, Stream Size: 486

| General | |
|---|---|
| Stream Path: | VBA/dir |
| File Type: | data |
| Stream Size: | 486 |
| Entropy: | 6.292426243264921 |
| Base64 Encoded: | True |
| Data ASCII: | ..........0.... ..H...........Project.Q.(..@.....=....l........APd-...".<....rstdo.le>..s.t..d.o.l.e.(..h..' ..*\\.G{00020430-....C.....46}#2.0#.0#C:\\Win.dows\\sys@tem32\\.e2..tlb#OLE. Automat.ion.ENor(malENCr.m.aF.. cEC....>m.! OfficgO.f.i.cg..g2DF8D0.4C-5BFA |
| Data Raw: | 01 e2 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 41 50 f4 64 2d 00 0c 02 22 0a 3c 02 0a 16 02 72 73 74 64 6f 08 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 00 28 0d 00 68 00 11 5e 00 03 2a 5c 00 47 7b 30 30 30 |

# Network Behavior

## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Aug 12, 2022 00:19:59.997840881 CEST | 49171 | 80 | 192.168.2.22 | 45.8.146.139 |
| Aug 12, 2022 00:20:03.007138968 CEST | 49171 | 80 | 192.168.2.22 | 45.8.146.139 |
| Aug 12, 2022 00:20:09.044693947 CEST | 49171 | 80 | 192.168.2.22 | 45.8.146.139 |
| Aug 12, 2022 00:20:21.058916092 CEST | 49172 | 80 | 192.168.2.22 | 45.8.146.139 |
| Aug 12, 2022 00:20:24.068888903 CEST | 49172 | 80 | 192.168.2.22 | 45.8.146.139 |
| Aug 12, 2022 00:20:30.075438976 CEST | 49172 | 80 | 192.168.2.22 | 45.8.146.139 |

# Statistics

⊘ **No statistics**

# System Behavior

## Analysis Process: WINWORD.EXE PID: **1056**, Parent PID: **576**

### General

| | |
|---|---|
| Target ID: | 0 |
| Start time: | 00:20:09 |
| Start date: | 12/08/2022 |
| 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: | 0x13f310000 |
| 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 | 6E062B14 | CreateDirectoryA |

#### File Deleted

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\~DFDF9B80FF6A2BA1D4.TMP | success or wait | 1 | 6E0E0648 | unknown |
| C:\Users\user\Desktop\~$ame removed] file 08.11.2022.doc | success or wait | 1 | 6E0E0648 | unknown |

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

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

#### File Read

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Windows\Fonts\StaticCache.dat | unknown | 60 | success or wait | 1 | 6E3DA0EB | ReadFile |
| C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC | unknown | 1 | success or wait | 1 | 6DFD1925 | unknown |
| C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC | unknown | 4096 | success or wait | 1 | 6DFD1925 | unknown |
| C:\Users\user\Desktop\[name removed] file 08.11.2022.doc | 1871139 | 333 | success or wait | 2 | 6E0E0648 | unknown |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2197A182.png | 0 | 65536 | success or wait | 4 | 6E0E0648 | unknown |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E4BEFF9B.png | 0 | 65536 | success or wait | 2 | 6E0E0648 | unknown |

### Registry Activities

#### Key Created

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\VBA | success or wait | 1 | 6E0BA5E3 | RegCreateKeyExA |
| HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0 | success or wait | 1 | 6E0BA5E3 | RegCreateKeyExA |
| HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common | success or wait | 1 | 6E0BA5E3 | RegCreateKeyExA |
| HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options | success or wait | 1 | 6E0E0648 | unknown |

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency | success or wait | 1 | 6E0E0648 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery | success or wait | 1 | 6E0E0648 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\77D3B | success or wait | 1 | 6E0E0648 | 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\77D3B | 77D3B | binary | 04 00 00 00 20 04 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 BC E7 FA 22 1C AE D8 01 3B 7D 07 00 3B 7D 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 | success or wait | 1 | 6E0E0648 | 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 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 | 1426849821 | success or wait | 1 | 6DFD1925 | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage | SpellingAndGrammarFiles_3082 | dword | 1426849821 | 1426849822 | success or wait | 1 | 6DFD1925 | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage | SpellingAndGrammarFiles_1036 | dword | 1358626844 | 1426849821 | success or wait | 1 | 6DFD1925 | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage | SpellingAndGrammarFiles_1036 | dword | 1426849821 | 1426849822 | success or wait | 1 | 6DFD1925 | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400100000000F01FEC\Usage | SpellingAndGrammarFiles_1033 | dword | 1358626865 | 1426849842 | success or wait | 1 | 6DFD1925 | 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\00004109F1009040010000 0000F01FEC\Usage | SpellingAndGrammarFiles_1033 | dword | 1426849842 | 1426849843 | success or wait | 1 | 6DFD1925 | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00004109F100A0C0010000 0000F01FEC\Usage | SpellingAndGrammarFiles_3082 | dword | 1426849822 | 1426849823 | success or wait | 1 | 6DFD1925 | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00004109F100A0C0010000 0000F01FEC\Usage | SpellingAndGrammarFiles_3082 | dword | 1426849823 | 1426849824 | success or wait | 1 | 6DFD1925 | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00004109F100C040010000 0000F01FEC\Usage | SpellingAndGrammarFiles_1036 | dword | 1426849822 | 1426849823 | success or wait | 1 | 6DFD1925 | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00004109F100C040010000 0000F01FEC\Usage | SpellingAndGrammarFiles_1036 | dword | 1426849823 | 1426849824 | success or wait | 1 | 6DFD1925 | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00004109F1009040010000 0000F01FEC\Usage | SpellingAndGrammarFiles_1033 | dword | 1426849843 | 1426849844 | success or wait | 1 | 6DFD1925 | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00004109F1009040010000 0000F01FEC\Usage | SpellingAndGrammarFiles_1033 | dword | 1426849844 | 1426849845 | success or wait | 1 | 6DFD1925 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\77D3B | 77D3B | binary | 04 00 00 00 20 04 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 BC E7 FA 22 1C AE D8 01 3B 7D 07 00 3B 7D 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 20 04 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 3B 7D 07 00 3B 7D 07 00 00 00 00 00 DB 04 00 00 00 00 00 | success or wait | 1 | 6E0E0648 | unknown |

| Key Path | Name | Type | Old Data | New Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| | | | FF FF FF FF 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>FF FF FF FF 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>00 00 00 00 00 00 00<br>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 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 FF FF FF FF |  |  |  |  |

## Disassembly

⊘ **No disassembly**