



ID: 715093

Sample Name: I6C8uDXVRN

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 16:13:43 Date: 03/10/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

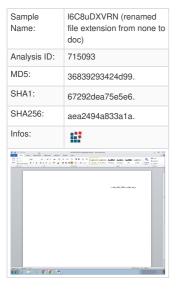
	2
Windows Analysis Report I6C8uDXVRN	3
Overview	3
General Information	3
Detection	
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Signatures	3
Sigma Signatures	3
Snort Signatures	3
Joe Sandbox Signatures	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files Unpacked PE Files	5
Domains	
URLs	· · · · · · · · · · · · · · · · · · ·
Domains and IPs	6
Contacted Domains	6
World Map of Contacted IPs	6
General Information	6
Warnings	7
Simulations	
Behavior and APIs	7
Joe Sandbox View / Context IPs	
Domains	· · · · · · · · · · · · · · · · · · ·
ASNs	
JA3 Fingerprints	7
Dropped Files	7
Created / dropped Files	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111A	47348ED}.tmp7
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111AC:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724AE5-A188-1111AC:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724AE5-A188-1111AC:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724AE5-A188-1111AC:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content\User\User\AppData\Local\Windows\Temporary Internet Files\Content\User\User\User\User\User\User\User\User	.47348ED}.tmp7 17141916}.tmp8
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111A	.47348ED}.tmp7 17141916}.tmp 8 8
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111AC:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724C:\Users\user\AppData\Local\Temp\~DFD655BEB157FA8F8B.TMP	.47348ED}.tmp7 17141916}.tmp 8 8
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111AC:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724C:\Users\user\AppData\Local\Temp\~DFD655BEB157FA8F8B.TMPC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.datC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\iffC8uDXVRN.LNKC:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm	.47348ED}.tmp7 !7141916}.tmp 8 8 8 8 8
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111AC:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724C:\Users\user\AppData\Local\Temp\~DFD655BEB157FA8F8B.TMPC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.datC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\l6C8uDXVRN.LNKC:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotmC:\Users\user\Desktop\~\$C8uDXVRN.doc	.47348ED}.tmp7 !7141916}.tmp 8 8 8 8 8 9
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111AC:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724C:\Users\user\AppData\Local\Temp\~DFD655BEB157FA8F8B.TMPC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.datC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\i6C8uDXVRN.LNKC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\i6C8uDXVRN.LNKC:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotmC:\Users\user\Desktop\~\$C8uDXVRN.docStatic File Info	.47348ED}.tmp7 I7141916}.tmp 8 8 8 8 9 9
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111AC:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724C:\Users\user\AppData\Local\Temp\~DFD655BEB157FA8F8B.TMPC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.datC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\i6C8uDXVRN.LNKC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\i6C8uDXVRN.LNKC:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotmC:\Users\user\Desktop\~\$C8uDXVRN.docStatic File InfoGeneral	.47348ED}.tmp7 !7141916}.tmp 8 .8 .8 .9 .9 .9 .9
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111AC:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724C:\Users\user\AppData\Local\Temp\~DFD655BEB157FA8F8B.TMPC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.datC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\i6C8uDXVRN.LNKC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\i6C8uDXVRN.LNKC:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotmC:\Users\user\Desktop\~\$C8uDXVRN.docStatic File Info	.47348ED}.tmp78.17141916}.tmp 8 .8 8 .8 9 .9 9 .9 9 .10
C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111AC:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724C:\Users\user\AppData\Loca\Temp\~DFD655BEB157FA8F8B.TMPC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.datC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.datC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.datC:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotmC:\Users\user\Desktop\~\$C8uDXVRN.docStatic File Info General File Icon Static OLE Info General	.47348ED}.tmp7 .7141916}.tmp 8 .8 .8 .8 .9 .9 .9 .9 .10 .10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111AC:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724C:\Users\user\AppData\Local\Temp\~DFD655BEB157FA8F8B.TMPC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.datC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\i6C8uDXVRN.LNKC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\i6C8uDXVRN.LNKC:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotmC:\Users\user\Desktop\~\$C8uDXVRN.docStatic File Info General File Icon Static OLE Info	.47348ED}.tmp7 .7141916}.tmp 8 .8 .8 .9 .9 .9 .9 .10 .10 .10
C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111AC:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724C:\Users\user\AppData\Loca\Temp\~DFD655BEB157FA8F8B.TMPC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.datC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.datC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.datC:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotmC:\Users\user\Desktop\~\$C8uDXVRN.docStatic File Info General File Icon Static OLE Info General OLE File "I6C8uDXVRN.doc" Indicators Summary	.47348ED}.tmp7 .7141916}.tmp 8 .8 .8 .8 .9 .9 .9 .10 .10 .10 .10 .10 .10 .10 .10 .10 .10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111AC:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724C:\Users\user\AppData\Local\Temp\~DFD655BEB157FA8F8B.TMPC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.datC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\i6C8uDXVRN.LNKC:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotmC:\Users\user\Desktop\~\$C8uDXVRN.doc} Static File Info General File Icon Static OLE Info General OLE File "I6C8uDXVRN.doc" Indicators Summary Document Summary Streams	.47348ED}.tmp78.17141916}.tmp 8
C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111A C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724} C:\Users\user\AppData\Loca\\Temp\~DFD655BEB157FA8F8B.TMP C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\l6C8uDXVRN.LNK C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm C:\Users\user\Desktop\~\$C8uDXVRN.doc Static File Info General File Icon Static OLE Info General OLE File "I6C8uDXVRN.doc" Indicators Summary Document Summary Streams Stream Path: \uxedocument Scream Size: 114 General Stream Path: \uxedocument Scream Size: 114 General	.47348ED}.tmp7 i7141916}.tmp 8 8 8 9 9 10 10 10 11 11 11
C:\Users\user\\appData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111A C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724} C:\Users\user\AppData\Local\Temp\~DFD655BEB157FA8F8B.TMP C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm C:\Users\user\Desktop\~\$C8uDXVRN.doc Static File Info General File Icon Static OLE Info General OLE File "I6C8uDXVRN.doc" Indicators Summary Document Summary Stream Stream Path: \ullCompObj, File Type: data, Stream Size: 4096 General Stream Path: \ullCompObj, File Type: data, Stream Size: 4096 General Stream Path: \ullCompObj, File Type: data, Stream Size: 4096 General	.47348ED}.tmp7 .7141916}.tmp 8 .8 .8 .9 .9 .10 .10 .10 .10 .10 .10 .10 .10 .10 .10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111A C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724} C:\Users\user\AppData\Local\Temp\~DFD655BEB157FA8F8B.TMP C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\under.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\under.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\under.dat C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm C:\Users\user\Desktop\~\$C8uDXVRN.doc Static File Info General File Icon Static OLE Info General OLE File "I6C8uDXVRN.doc" Indicators Summary Document Summary Document Summary Streams Stream Pafi:\ulder\under\u	.47348ED}.tmp7 .7141916}.tmp 8 .8 .8 .8 .9 .9 .9 .10 .10 .10 .10 .10 .10 .10 .10 .10 .10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111A C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724} C:\Users\user\AppData\Local\Temp\~DFD655BEB157FA8F8B.TMP C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm C:\Users\user\Desktop\~\$C8uDXVRN.doc Static File Info General File Icon Static OLE Info General OLE File "I6C8uDXVRN.doc" Indicators Summary Document Summary Document Summary Streams Stream Paff: \under\Compobj, File Type: data, Stream Size: 4096 General Stream Paff: \under\Compobj, File Type: data, Stream Size: 4096 General Stream Paff: \under\Compobj, File Type: data, Stream Size: 4096 General Stream Paff: \under\Compobj, File Type: data, Stream Size: 4096 General Stream Paff: \under\Compobj, File Type: data, Stream Size: 4096 General Stream Paff: \under\Compobj, File Type: data, Stream Size: 4096 General Stream Paff: \under\Compobj, File Type: data, Stream Size: 4096 General Stream Paff: \under\Compobj, File Type: data, Stream Size: 4096 General Stream Paff: \under\Compobj, File Type: data, Stream Size: 4096 General	47348ED}.tmp7 47141916}.tmp 8 8 8 8 9 9 9 10 10 10 11 11 11 11 11 11 11 11 11 11
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111A C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724} C:\Users\user\AppData\Local\Temp\~DF0655BEB157FA8F8B.TMP C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\local\Csup\Csup\Users\user\AppData\Roaming\Microsoft\Office\Recent\local\Csup\Users\user\AppData\Roaming\Microsoft\Office\Recent\local\Csup\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm C:\Users\user\Desktop\~\$C8uDXVRN.doc Static File Info General File Icon Static OLE Info General OLE File "I6C8uDXVRN.doc" Indicators Summary Document Summary Stream Stream Path: v1CompObj, File Type: data, Stream Size: 114 General Stream Path: v1CompObj, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General	47348ED}.tmp7817141916}.tmp888888888888888888888888888888888888
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111A C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724} C:\Users\user\AppData\Local\Temp\~DFD655BEB157FA8F8B.TMP C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.at C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.at C:\Users\user\Desktop\~\$C8uDXVRN.doc C:\Users\user\Desktop\~\$C8uDXVRN.doc Static File Info General File Icon Static OLE Info General OLE File "I6C8uDXVRN.doc" Indicators Surmany Document Summary Document Summary Stream Stream Path: vtCompObj, File Type: data, Stream Size: 4096 General Stream Path: vtSoummaryInformation, File Type: data, Stream Size: 4096 General Stream Path: vtSoummaryInformation, File Type: data, Stream Size: 4096 General Stream Path: vtGobocument, File Type: data, Stream Size: 4096 General Stream Path: vtGobocument, File Type: data, Stream Size: 4096 General Stream Path: vtGobocument, File Type: data, Stream Size: 4096 General Stream Path: vtGobocument, File Type: data, Stream Size: 4096 General Stream Path: vtGobocument, File Type: data, Stream Size: 4096 General Stream Path: vtGobocument, File Type: data, Stream Size: 4096 General Stream Path: vtGobocument, File Type: data, Stream Size: 4096 General Stream Path: vtGobocument, File Type: data, Stream Size: 4096 General	17141916}.tmp78 17141916}.tmp78 18 18 19 10 10 10 11 11 11 11 11 11 11 11 11 11
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111A C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724} C:\Users\user\AppData\Local\Temp\~DF0655BEB157FA8F8B.TMP C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\local\Csup\Csup\Users\user\AppData\Roaming\Microsoft\Office\Recent\local\Csup\Users\user\AppData\Roaming\Microsoft\Office\Recent\local\Csup\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm C:\Users\user\Desktop\~\$C8uDXVRN.doc Static File Info General File Icon Static OLE Info General OLE File "I6C8uDXVRN.doc" Indicators Summary Document Summary Stream Stream Path: v1CompObj, File Type: data, Stream Size: 114 General Stream Path: v1CompObj, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General Stream Path: v1CompObi, File Type: data, Stream Size: 4096 General	12 12
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111A C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724} C:\Users\user\AppData\Local\Temp\~DF0655BEB157FA8F8B.TMP C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.at C:\User\user\AppData\Roaming\Microsoft\Office\Recent\index.at C:\User\user\User\AppData\Roaming\Microsoft\Office\	12 12
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111A C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724} C:\Users\user\AppData\Local\Temp\~DF0655BEB157FA8F8B.TMP C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.adt File Info General File Info General OLE File 'li6'\user\user\user\AppData\Roaming\Microsoft\Office\Recent\user\user\AppBata\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office\Roaming\Microsoft\Office	.47348ED}.tmp7 .7141916}.tmp 8 .8 .8 .8 .9 .9 .9 .10 .10 .10 .10 .10 .10 .10 .10 .10 .10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111A C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724} C:\Users\user\AppData\Local\Temp\~DF0655BEB157FA8F8B.TMP C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.at C:\User\user\AppData\Roaming\Microsoft\Office\Recent\index.at C:\User\user\User\AppData\Roaming\Microsoft\Office\	147348ED}.tmp7 17141916}.tmp 8 8 8 9 9 10 10 10 10 11 11 11 11 11 11 11 11 11
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF\(CF355214-6435-4AE5-A188-1111AC.\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS\(4B6588AD-3520-46EF-A143-38724C.\Users\user\AppData\Local\Temp\~DF0655BEB157FA8F8B.TMP C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\user\AppData\Roaming\Microsoft\Office\Recent\index.dotm C:\Users\user\user\AppData\Roaming\Microsoft\Office\Recent\index.dotm C:\Users\user\user\AppData\Roaming\Microsoft\Office\Recent\index.dotm C:\Users\user\user\AppData\Roaming\Microsoft\Office\Recent\index.dotm C:\Users\user\user\AppData\Roaming\Microsoft\Office\Recent\index.dotm C:\Users\user\user\AppData\Roaming\Microsoft\Office\Recent\index.dotm C:\Users\user\user\AppData\Roaming\Microsoft\Office\Recent\index.dotm C:\Users\user\user\AppData\Roaming\Microsoft\Office\Recent\index.dotm General Simmany DocumentSummany Siream Patr\user\undex.document\undex.price\undex.doff\Office\Roaming\Microsoft\Office\Roaming\R	147348ED}.tmp787141916}.tmp787141916}.tmp7888888888888888888888888888888888888
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF\(CF355214-6435-4AE5-A188-1111AC:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS\(4B6588AD-3520-46EF-A143-38724C:\Users\user\AppData\Local\Temp\~PDF655BE157FA8F8B.TMP C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.Adm C:\Users\user\Dpsta\Roaming\Microsoft\Office\Recent\index.P\something\Temp\	10 10 10 10 10 10 10 10 10 10 10 10 10 1
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111A C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-38724} C:\Users\user\AppData\Local\Temp\~DF055BEB157FA8F8B.TMP C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm C:\Users\user\AppData\Roaming\Microsoft\Templates\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	

Windows Analysis Report

l6C8uDXVRN

Overview

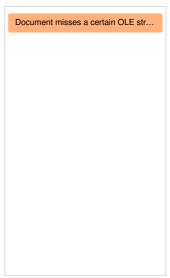
General Information



Detection



Signatures



Classification



Process Tree

- System is w7x64
- WINWORD.EXE (PID: 1708 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

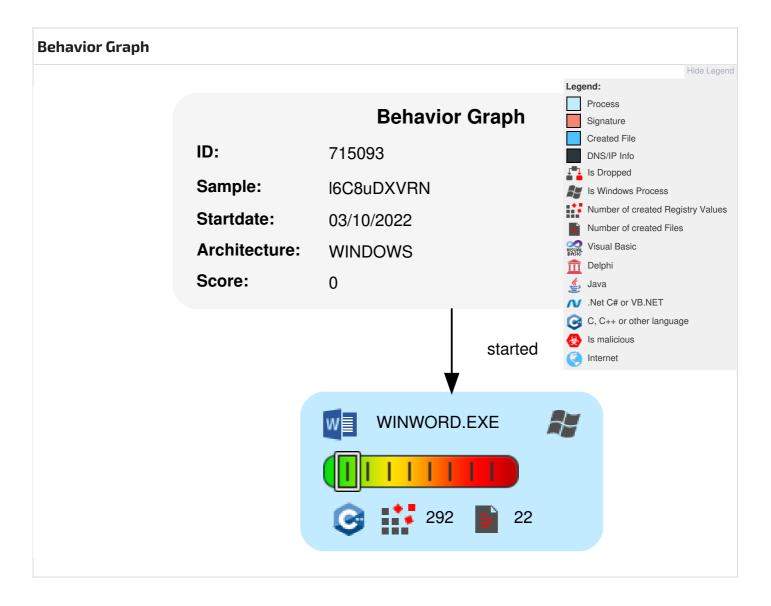
No Snort rule has matched

Copyright Joe Security LLC 2022 Page 3 of 17

Joe Sandbox Signatures

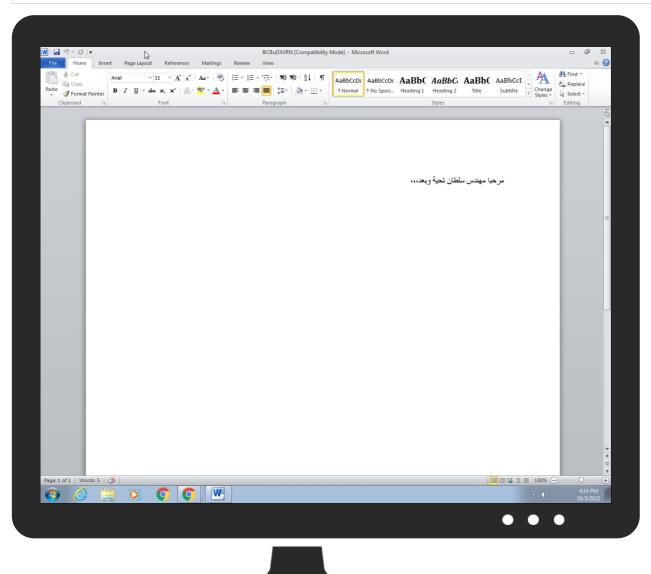
There are no malicious signatures, click here to show all signatures

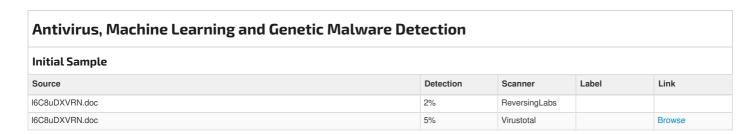
Mitre	Mitre Att&ck Matrix												
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Manageme nt Instrument ation	Path Interceptio n	Path Interceptio n	1 Masqueradi ng	OS Credential Dumping	File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer	Eavesdrop on Insecure Network Communic ation	Remotely Track Device Without Authorizati on	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initializatio n Scripts	Boot or Logon Initializatio n Scripts	Rootkit	LSASS Memory	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 Authorizati on	Device Lockout



Copyright Joe Security LLC 2022 Page 4 of 17

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





Dropped Files

Copyright Joe Security LLC 2022 Page 5 of 17

\oslash	No Antivirus matches
-----------	----------------------

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

HCA Information:

General Information Joe Sandbox Version: 36.0.0 Rainbow Opal Analysis ID: 715093 Start date and time: 2022-10-03 16:13:43 +02:00 Joe Sandbox Product: CloudBasic Overall analysis duration: 0h 4m 28s Hypervisor based Inspection enabled: false light Report type: Sample file name: I6C8uDXVRN (renamed file extension from none to 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 3 analysed: Number of new started drivers analysed: 0 Number of existing processes analysed: 0 Number of existing drivers analysed: 0 0 Number of injected processes analysed: HCA enabled Technologies: • EGA enabled HDC enabled AMSI enabled Analysis Mode: default Analysis stop reason: Timeout Detection: CLEAN Classification: clean0.winDOC@1/7@0/0 HDC Information: Failed

Copyright Joe Security LLC 2022 Page 6 of 17

Successful, ratio: 100%
Number of executed functions: 0
Number of non-executed functions: 0

Cookbook Comments:	Found Word or Excel or PowerPoint or XPS Viewer
	Attach to Office via COM
	Scroll down
	Close Viewer

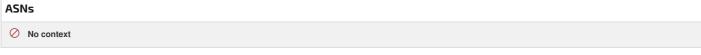
Warnings

- Exclude process from analysis (whitelisted): dllhost.exe
 Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations Behavior and APIs No simulations

Joe Sandbox View / Context	
IPs	
⊘ No context	
Domains	

⊘ No context



JA3 Fingerprints	
⊘ No context	

Dropped Files	
On context	

Created	Created / dropped Files			
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111A47348ED}.tmp				
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE			
File Type:	Composite Document File V2 Document, Cannot read section info			
Category:	dropped			
Size (bytes):	2560			
Entropy (8bit):	1.4315306186905608			
Encrypted:	false			
SSDEEP:	12:rl3lTpFQhluMOEt4Clht4ht4ClClCb77:rn/Q			
MD5:	8862D7FAF983D2906280AA79BE4B5E67			
SHA1:	7C91EE4D2700CDE20923814DAC449117F71D3BFE			
SHA-256:	678E55AB32A981A765E8E467056F7CEECA3FDF19DA28C8899DEB3364F47D81C9			
SHA-512:	6C31777F2F131ADE771E8C1B2C8052D98D96A878F413A594998AC01928F3D73114FA187C7E09C37856DFF5C191286C8C64A0CAA9170BDBAEBBECC8B838CFF			
Malicious:	false			
Reputation:	low			

Copyright Joe Security LLC 2022 Page 7 of 17

Preview:	

C:\Users\use	r\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-387247141916}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F26A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	

C:\Users\use	r\AppData\Local\Temp\~DFD655BEB157FA8F8B.TMP
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat		
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE	
File Type:	Generic INItialization configuration [doc]	
Category:	dropped	
Size (bytes):	71	
Entropy (8bit):	4.778504211951284	
Encrypted:	false	
SSDEEP:	3:bDuMJIRn3rpFomX1dqa3rpFov:bCab3t3y	
MD5:	9381283F1A2063D0EF0C1DE1E05B626A	
SHA1:	CC9BDE1D52EC9642243399FF41EAC45A5546293F	
SHA-256:	BD573ECC9C5BF91A12107F2C4FE543A1E45683ECAA8E45836B6709F1E4183656	
SHA-512:	FEC581E206327F305749C9691D8FED304FB2D3856AABB94F25E12BD23CB711E639DBEA75A3162932E239E8AF151CFE34F7E9A1F26D14A921321C6DC3E7E8ACE8	
Malicious:	false	
Reputation:	low	
Preview:	[folders]Templates.LNK=0I6C8uDXVRN.LNK=0[doc]I6C8uDXVRN.LNK=0	

C: Users AppData Roaming Microsoft Office Recent L6C8uDXVRN.LNK

Copyright Joe Security LLC 2022 Page 8 of 17

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=Mon Oct 3 22:14:06 2022, mtime=Mon Oct 3 22:14:	
Category:	dropped	
Size (bytes):	1014	
Entropy (8bit):	4.512031842789759	
Encrypted:	false	
SSDEEP:	12:8190FgXg/XAICPCHaXNBQtB/uUgX+WvkcCFcdiSnicvb7Ai2S5DtZ3YilMMEpxRW:83w/XT9S0n0Fcd4evA2Dv3qwtiu7D	
MD5:	EB5F7A08684E47A76C23108ECD7F8A96	
SHA1:	D40DC2E8FC8CC6E6A685E9EC39D25F84D3CEAAC1	
SHA-256:	15DCF99443C8912CBB181D18034E96F8A2AFAAD2F62D720EDE290D472A5FEDD9	
SHA-512:	FDF5D8A811F290EF330E9B5A5D7AB0A49B6505975CC6D6506F1AC5C7B08E6F5B8688B4E576BED5B56171FE2708E52FFE50DE10D195AA6F57DF50E89A7FB40C45	
Malicious:	false	
Reputation:	low	
Preview:	L	

C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm		
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE	
File Type:	data	
Category:	dropped	
Size (bytes):	162	
Entropy (8bit):	2.503835550707525	
Encrypted:	false	
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll	
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9	
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1	
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11	
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265	
Malicious:	false	
Reputation:	moderate, very likely benign file	
Preview:	.user	

C:\Users\user\Desktop\~\$C8uDXVRN.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265
Malicious:	false
Preview:	.user

Static File Info

General

File type:

Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Author: ayman alkhateeb, Template: Normal.dotm, Last Saved By: ayman alkhateeb, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Total Editing Time: 01:00, Create Time/Date: Sun Oct 2 11:52:00 2022, Last Saved Time/Date: Sun Oct 2 11:53:00 2022, Number of Pages: 1, Number of Words: 4, Number of Characters: 27, Security: 0

Copyright Joe Security LLC 2022 Page 9 of 17

Entropy (8bit):	2.9464620025743873
TrID:	 Microsoft Word document (32009/1) 54.23% Microsoft Word document (old ver.) (19008/1) 32.20% Generic OLE2 / Multistream Compound File (8008/1) 13.57%
File name:	I6C8uDXVRN.doc
File size:	22528
MD5:	36839293424d99142586e6afd07b3260
SHA1:	67292dea75e5e63254cbe39e6a8d0b60479270b2
SHA256:	aea2494a833a1ad438574250b3132746a0055a84ee9c09964a6776c2d18dd427
SHA512:	503b477daac01f0c3f0e7b50bac7cd589f9b64c335ea4f2f373d0d99c9706b254734f3e08289a5d54dbc7e984799376efe904b76ee88a9dc05184c55180f2bff
SSDEEP:	96: wDDhElLZDQvA+6Zjp6bfu+RxCL7kzmzpxjK93ytK3HCHXWxFpgNMsAL4qab+ptjR: w/ulLZEvA+6/6rrlLd/Kf3HO8tsHwJA
TLSH:	1AA2EA46B2D5CD5AF22601B08947C3C4722DBE6D5E16C24B7B643F2EFCB12B14A36749
File Content Preview:	

File Icon



e4eea2aaa4b4b4a4

Static OLE Info

General

OLE Document Type: Number of OLE Files: 1

OLE File "l6C8uDXVRN.doc"

Indicators

Has Summary Info: Microsoft Office Word Application Name: Encrypted Document: False Contains Word Document Stream: Contains Workbook/Book Stream: False Contains PowerPoint Document False Stream: Contains Visio Document Stream: False Contains ObjectPool Stream: False Flash Objects Count: 0 Contains VBA Macros: False

Summary	
Code Page:	1252
Title:	
Subject:	
Author:	
Keywords:	
Comments:	
Template:	
Last Saved By:	
Revion Number:	1
Total Edit Time:	60
Create Time:	2022-10-02 10:52:00
Last Saved Time:	2022-10-02 10:53:00
Number of Pages:	1
Number of Words:	4
Number of Characters:	27
Creating Application:	
Security:	0

Document Summary	
Document Code Page:	1252
Number of Lines:	1

Copyright Joe Security LLC 2022 Page 10 of 17

Number of Paragraphs:	1
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	983040

Stream Path: \x1CompObj, File Type: data, Stream Size: 114	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.235956365095031
Base64 Encoded:	True
Data ASCII:	FMicrosoft Word 97-2003 DocumentMSWordDocWord.Document.8.9q.
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 06 09 02 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5Docume	Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096	
General		
Stream Path:	\x5DocumentSummaryInformation	
File Type:	data	
Stream Size:	4096	
Entropy:	0.24406859507157763	
Base64 Encoded:	False	
Data ASCII:		
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00	

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 General	
File Type:	data
Stream Size:	4096
Entropy:	0.5149245210202502
Base64 Encoded:	False
Data ASCII:	Oh+'0
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 6874	
General	
Stream Path:	1Table
File Type:	data
Stream Size:	6874
Entropy:	5.90667362609459
Base64 Encoded:	True
Data ASCII:	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$
Data Raw:	0e 06 0f 00 12 00 01 00 73 01 0f 00 07 00 03 00 03 00 03 00 02 00 04 00 08 00 00 09 8 00 00 09 e 00 00 09 e 00 00 09 e 00 00 09 e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00

Stream Path: WordDocument, File Type: data, Stream Size: 4096

Copyright Joe Security LLC 2022 Page 11 of 17

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	4096
Entropy:	1.2676117739723565
Base64 Encoded:	False
Data ASCII:	.[0>bjbjpa!\\pa!\\666
Data Raw:	ec a5 c1 00 5b e0 09 04 00 00 f0 12 bf 00 00 00 00 00 00 00 00 00 00 00 00 00

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 1708, Parent PID: 576

Anatysis i rocess.	WINVEND.EXC TO THE PROPERTY OF				
General					
Target ID:	0				
Start time:	16:14:16				
Start date:	03/10/2022				
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:	0x13f410000				
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	6DD62B14	CreateDirect oryA			

File Path						Completion	Co	ount	Source Address	Symbol
Old File Path	New File Path Comp				Comple	etion	Count	Sou	rce Address	Symbol
File Path	Offset	Length	Value	Ascii		Completion	_	ount	Source Address	Symbol

Copyright Joe Security LLC 2022 Page 12 of 17

Registry Activities				
Key Created				
Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6DDBA5E3	RegCreateKeyEx A
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6DDBA5E3	RegCreateKeyEx A
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6DDBA5E3	RegCreateKeyEx A
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6DDE0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6DDE0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6DDE0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\6DC89	success or wait	1	6DDE0648	unknown

HKEY_CURRENT_USER\Software	\Microsoft\Office\1	4.0\Word\Resilienc	y\DocumentRecovery\6DC89	success or wait	1 (6DDE0648	unknown
Key Value Created							
Key Path	Name	Туре	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Softwar e\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	6DDE0648	unknown
etwicrosoft\Shared Tools\Panose HKEY_CURRENT_USER\Softwar etwicrosoft\Office\14.0\Word\Resili ency\DocumentRecovery\6DC89	6DC89	binary	04 00 00 00 AC 06 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 6C 00 62 00 75 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 6C 00 62 00 67 00 73 00 5C 00 41 00 6C 00 5C 00 44 00 61 00 74 00 61 00 5C 00 5C 00 54 00 65 00 6D 00 70 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 60 00 60 00 00 00 00 00 00 00 00 00		1	6DDE0648	unknown

Key Path	Name	Туре	00 00 00 00 00 00 00 00 00 00 00 00 00	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 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	Туре	Old Data	New Data	Completion	Count	Source Address	Symbol	
HKEY_LOCAL_MACH INE\SOFTWARE\Mi crosoft\Windows\Curre ntVersion \Installer\UserData\S- 1-5-18\P roducts\00004109D30 00000010000 0000F01FEC\Usage	ProductFiles	dword	1430454321	1430454322	success or wait	1	6DDE0648	unknown	
HKEY_LOCAL_MACH INE\SOFTWARE\Mi crosoft\Windows\Curre ntVersion .Installer\UserData\S- 1-5-18\P roducts\00004109D30 00000010000 0000F01FEC\Usage	ProductFiles	dword	1430454322	1430454323	success or wait	1	6DDE0648	unknown	
HKEY_CURRENT_US ER\Software\Mic rosoft\Office\14.0\Wor d\Resili ency\DocumentRecov ery\6DC89	6DC89	binary	04 00 00 00 AC 06 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	04 00 00 00 AC 06 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	success or wait	1	6DDE0648	unknown	

Copyright Joe Security LLC 2022 Page 14 of 17

Key Path	Name	Туре	69 00 6D 00 67 00 73 00 2HdD 3 00 74 00 6D 00 04 00 00 00 69 00 6D 00	54 00 65 00 6D 00 70 New Data 69 00 6D 00 67 00 73 00 2E 00 68	Completion	Count	Source Address	Symbol
			67 00 73 00 00 00 00 00	00 74 00 6D 00 04 00				
			01 00 00 00 00 00 00 00	00 00 69 00 6D 00 67				
			74 FD 1C EE 7D D7 D8 01	00 73 00 00 00 00 00				
			89 DC 06 00 89 DC 06 00	01 00 00 00 00 00 00				
			00 00 00 00 DB 04 00 00	00 00 00 00 00 00 00				
			02 00 00 00 00 00 00 00	00 00 89 DC 06 00 89				
			00 00 00 00 00 00 00 00	DC 06 00 00 00 00 00				
			00 00 00 00 00 00 00 00	DB 04 00 00 02 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	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 0	00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00 0				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00 0				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00 0				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	$\begin{array}{cccccccccccccccccccccccccccccccccccc$				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	$\begin{array}{cccccccccccccccccccccccccccccccccccc$				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00 0				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00 0				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	$\begin{array}{c} 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	$\begin{array}{cccccccccccccccccccccccccccccccccccc$				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	$\begin{array}{c} 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$				

Copyright Joe Security LLC 2022 Page 15 of 17

Key Path	Name	Туре	刻ゆか時 00 00 00 00 00 00 刻ゆか時 00 00 00 00 00 00	96.00 00 00 00 00 00 00 00 00 00 00 00 00 	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00				
			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				

Copyright Joe Security LLC 2022

Key Path	Name	Туре	Old Data	00 00 00 00 00 00 00 612 60 10 10 10 10 10 10 10 1	Completion	Count	Source Address	Symbol
				00 00 00 00 00 00 00 00 00 00 00 00 00 0				
				00 00 00 00 00 00 00 00 00 00 00 FF FF FF				

Disassembly



No disassembly

Copyright Joe Security LLC 2022 Page 17 of 17