

JOESandbox Cloud BASIC



**ID:** 715093

**Sample Name:** l6C8uDXVRN

**Cookbook:**

defaultwindowsofficecookbook.jbs

**Time:** 16:13:43

**Date:** 03/10/2022

**Version:** 36.0.0 Rainbow Opal

# Table of Contents


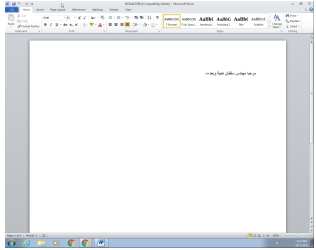
Table of Contents	2
Windows Analysis Report I6C8uDXVRN	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Signatures	3
Sigma Signatures	3
Snort Signatures	3
Joe Sandbox Signatures	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	5
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	6
Contacted Domains	6
World Map of Contacted IPs	6
General Information	6
Warnings	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	7
IPs	7
Domains	7
ASNs	7
JA3 Fingerprints	7
Dropped Files	7
Created / dropped Files	7
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{CF355214-6435-4AE5-A188-1111A47348ED}.tmp	7
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4B6588AD-3520-46EF-A143-387247141916}.tmp	8
C:\Users\user\AppData\Local\Temp\~DFD655BEB157FA8F8B.TMP	8
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	8
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\I6C8uDXVRN.LNK	8
C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm	9
C:\Users\user\Desktop\~\$C8uDXVRN.doc	9
Static File Info	9
General	9
File Icon	10
Static OLE Info	10
General	10
OLE File "I6C8uDXVRN.doc"	10
Indicators	10
Summary	10
Document Summary	10
Streams	11
Stream Path: \x1CompObj, File Type: data, Stream Size: 114	11
General	11
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096	11
General	11
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096	11
General	11
Stream Path: 1Table, File Type: data, Stream Size: 6874	11
General	11
Stream Path: WordDocument, File Type: data, Stream Size: 4096	11
General	12
Network Behavior	12
Statistics	12
System Behavior	12
Analysis Process: WINWORD.EXEPID: 1708, Parent PID: 576	12
General	12
File Activities	12
File Created	12
Registry Activities	13
Key Created	13
Key Value Created	13
Key Value Modified	14
Disassembly	17

# Windows Analysis Report

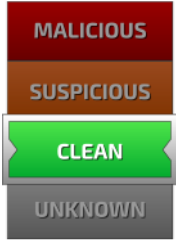
I6C8uDXVRN

## Overview

### General Information

Sample Name:	I6C8uDXVRN (renamed file extension from none to doc)
Analysis ID:	715093
MD5:	36839293424d99.
SHA1:	67292dea75e5e6.
SHA256:	aea2494a833a1a.
Infos:	
	

### Detection

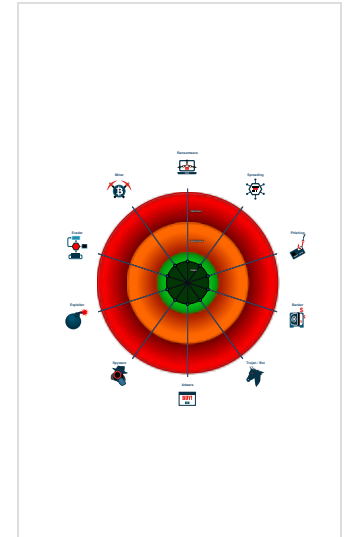


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

### Signatures

Document misses a certain OLE str...


### Classification



## Process Tree

- System is w7x64
-  WINWORD.EXE (PID: 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

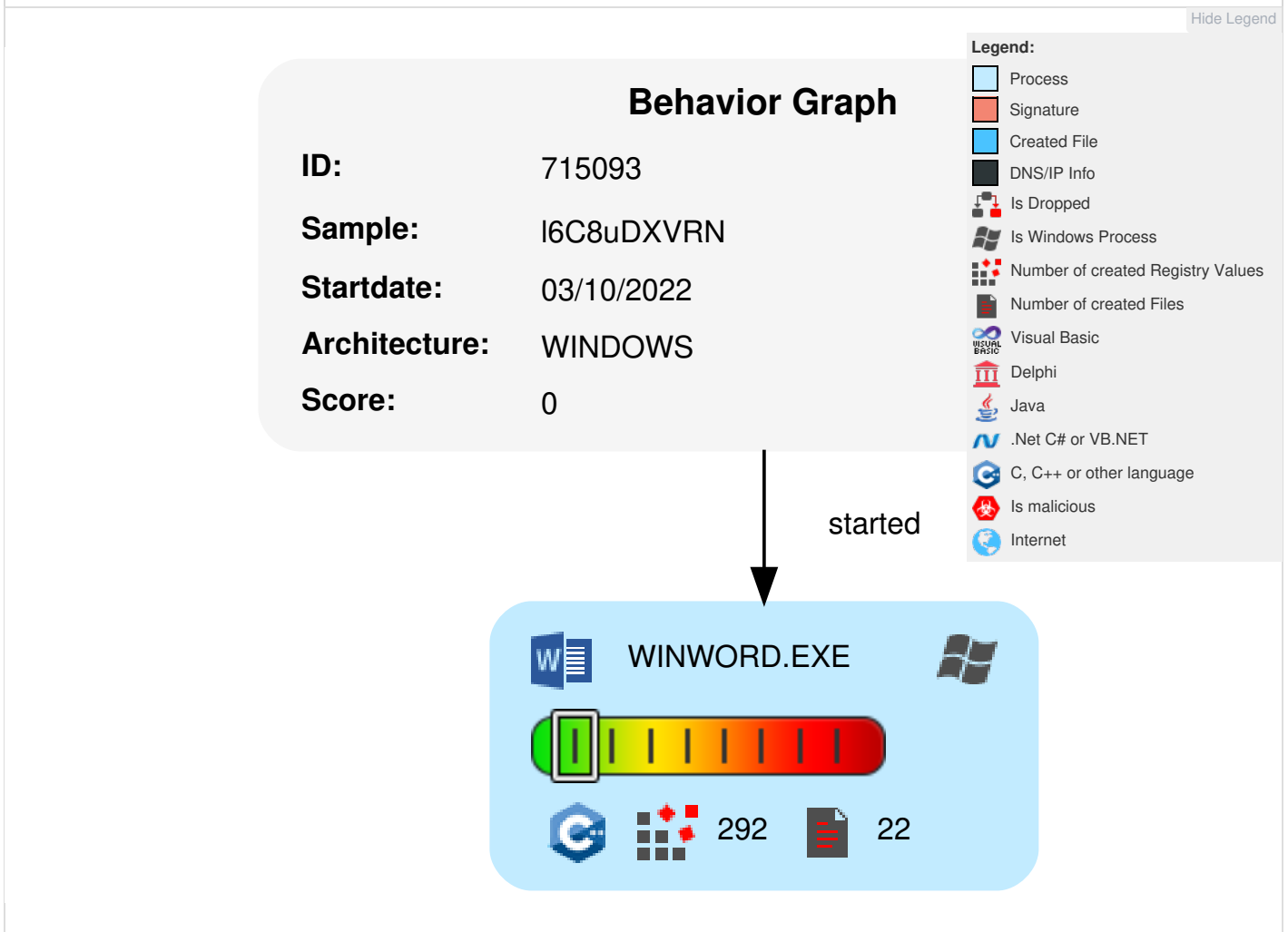
# Joe Sandbox Signatures

There are no malicious signatures, [click here to show all signatures](#).

## Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

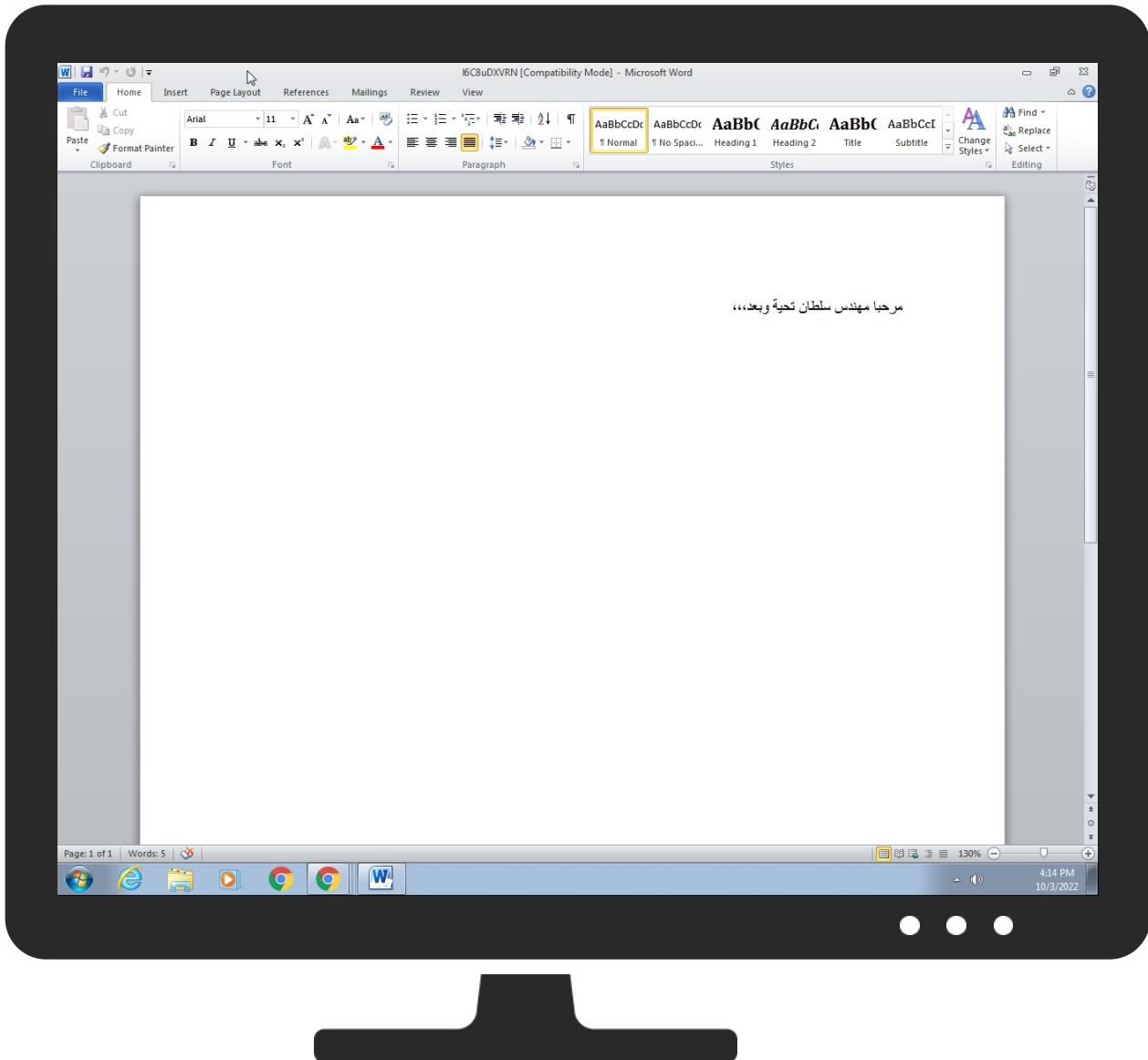
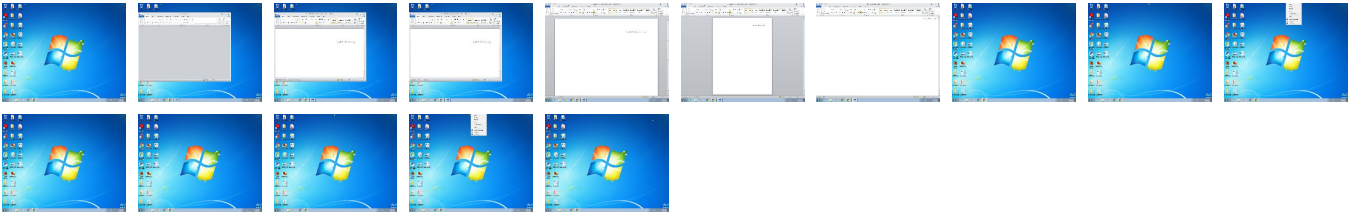
## Behavior Graph



## Screenshots

### Thumbnails

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



## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

Source	Detection	Scanner	Label	Link
I6C8uDXVRN.doc	2%	ReversingLabs		
I6C8uDXVRN.doc	5%	Virusotal		<a href="#">Browse</a>

### Dropped Files

⊘ No Antivirus matches

## Unpacked PE Files

⊘ No Antivirus matches

## Domains

⊘ No Antivirus matches

## URLs

⊘ No Antivirus matches

## Domains and IPs

### Contacted Domains

⊘ No contacted domains info

### World Map of Contacted IPs

⊘ No contacted IP infos

## General Information

Joe Sandbox Version:	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
Report type:	light
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 analysed:	3
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	<ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winDOC@1/7@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 100%</li><li>• Number of executed functions: 0</li><li>• Number of non-executed functions: 0</li></ul>


Cookbook Comments:	<ul style="list-style-type: none"> <li>• Found Word or Excel or PowerPoint or XPS Viewer</li> <li>• Attach to Office via COM</li> <li>• Scroll down</li> <li>• Close Viewer</li> </ul>
--------------------	--

## Warnings

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


## Simulations

### Behavior and APIs


 No simulations

## Joe Sandbox View / Context


### IPs

 No context


### Domains

 No context


### ASNs

 No context

### JA3 Fingerprints

 No context

### Dropped Files

 No context

## Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.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:rI3ITpFQhluMOEt4uMOEt4CIht4ht4CICICb77:m/Q
MD5:	8862D7FAF983D2906280AA79BE4B5E67
SHA1:	7C91EE4D2700CDE20923814DAC449117F71D3BFE
SHA-256:	678E55AB32A981A765E8E467056F7CEECA3FDF19DA28C8899DEB3364F47D81C9
SHA-512:	6C31777F2F131ADE771E8C1B2C8052D98D96A878F413A594998AC01928F3D73114FA187C7E09C37856DFF5C191286C8C64A0CAA9170BDBAEBBECC8B838CFF34
Malicious:	false
Reputation:	low

Preview:	.....>..... ..... ..... .....
----------	--

<b>C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\--WRS{4B6588AD-3520-46EF-A143-387247141916}.tmp</b>	
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:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBCECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..... ..... .....

<b>C:\Users\user\AppData\Local\Temp\--DFD655BEB157FA8F8B.TMP</b>	
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:	..... .....

<b>C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat</b>	
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:bDuMJIRn3rpFomX1dq3rpFov:bCab3t3y
MD5:	9381283F1A2063D0EF0C1DE1E05B626A
SHA1:	CC9BDE1D52EC9642243399FF41EAC45A5546293F
SHA-256:	BD573ECC9C5BF91A12107F2C4FE543A1E45683ECAA8E45836B6709F1E4183656
SHA-512:	FEC581E206327F305749C9691D8FED304FB2D3856AABB94F25E12BD23CB711E639DBEA75A3162932E239E8AF151CFE34F7E9A1F26D14A921321C6DC3E7E8ACE8
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..I6C8uDXVRN.LNK=0..[doc]..I6C8uDXVRN.LNK=0..

<b>C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\I6C8uDXVRN.LNK</b>	
---	--




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 22:14:06 2022, atime=Mon Oct 3 22:14:16 2022, length=22528, window=hide
Category:	dropped
Size (bytes):	1014
Entropy (8bit):	4.512031842789759
Encrypted:	false
SSDEEP:	12:8190FgXg/XAICPCHaXNBQIB/uUgX+WvkcCFodiSnicvb7Ai2S5DtZ3YiIMMEpxRW:83w/XT9S0n0Fcd4evA2Dv3qwtiu7D
MD5:	EB5F7A08684E47A76C23108ECD7F8A96
SHA1:	D40DC2E8FC8CC6E6A685E9EC39D25F84D3CEAAC1
SHA-256:	15D0CF99443C8912CBB181D18034E96F8A2AFAAD2F62D720EDE290D472A5FEDD9
SHA-512:	FDF5D8A811F290EF330E9B5A5D7AB0A49B6505975CC6D6506F1AC5C7B08E6F5B8688B4E576BED5B56171FE2708E52FFE50DE10D195AA6F57DF50E89A7FB40C45
Malicious:	false
Reputation:	low
Preview:	L.....F.....}.....}.....5:.....X.....P.O. ....+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....CU...Desktop.d....QK.XCU.*..._=.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....f.2..X..CU. .L6C8UD~1.DOC..J.....CU.CU.*.....I.6.C.8.u.D.X.V.R.N...d.o.c.....x.....8.....?J.....C:\Users\#.....\506013\User s.user\Desktop\l6C8uDXVRN.doc.%.....\.....\.....\D.e.s.k.t.o.p\l.6.C.8.u.D.X.V.R.N...d.o.c.....;..LB.)...Ag.....1SPS.XF.L8C...&.m.m.....S.-.1.-.5-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....X.....506013.....D_...3N...W...9G..N.....[D_...3N...W...9G..N..

<b>C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm</b>	
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:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F052655
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

<b>C:\Users\user\Desktop\~\$C8uDXVRN.doc</b>	
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:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F052655
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

<b>Static File Info</b>	
<b>General</b>	
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

Entropy (8bit):	2.9464620025743873
TrID:	<ul style="list-style-type: none"> <li>• Microsoft Word document (32009/1) 54.23%</li> <li>• Microsoft Word document (old ver.) (19008/1) 32.20%</li> <li>• Generic OLE2 / Multistream Compound File (8008/1) 13.57%</li> </ul>
File name:	I6C8uDXVRN.doc
File size:	22528
MD5:	36839293424d99142586e6afd07b3260
SHA1:	67292dea75e5e63254cbe39e6a8d0b60479270b2
SHA256:	aea2494a833a1ad438574250b3132746a0055a84ee9c09964a6776c2d18dd427
SHA512:	503b477daac01f0c3f0e7b50bac7cd589f9b64c335ea4f2f373d0d99c9706b254734f3e08289a5d54dbc7e984799376efe904b76ee88a9dc05184c55180f2bff
SSDEEP:	96:wDdhEILZDQvA+6Zjp6bfu+RxCL7kzmzpxjK93ytK3HCHXWxFpgNMsAL4qab+ptjR:w/uLLzEvA+6/6rrlLd/Kf3HO8tsHwJA
TLSH:	1AA2EA46B2D5CD5AF22601B08947C3C4722DBE6D5E16C24B7B643F2EFCB12B14A36749
File Content Preview:	.....>.....').....&.....

<b>File Icon</b>	
	
Icon Hash:	e4eea2aaa4b4b4a4

<b>Static OLE Info</b>	
<b>General</b>	
Document Type:	OLE
Number of OLE Files:	1

<b>OLE File "I6C8uDXVRN.doc"</b>	
<b>Indicators</b>	
Has Summary Info:	
Application Name:	Microsoft Office Word
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:	False

<b>Summary</b>	
Code Page:	1252
Title:	
Subject:	
Author:	
Keywords:	
Comments:	
Template:	
Last Saved By:	
Revision 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

<b>Document Summary</b>	
Document Code Page:	1252
Number of Lines:	1















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

Disassembly
⊘ No disassembly