ID: 332012
Sample Name: COVID-Trial-Application-Frm09874x.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 23:43:09
Date: 17/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

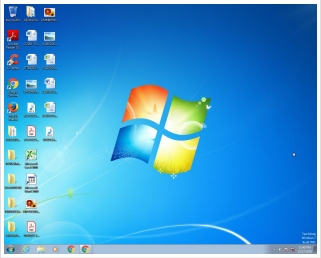
Analysis Report COVID-Trial-Application-Frm09874x.docx

Overview

General Information

Sample Name:	COVID-Trial-Application-Frm09874x.docx
Analysis ID:	332012
MD5:	0343741d7f9a129.
SHA1:	5aae176e9f1b983.
SHA256:	61e5c441089b95..

Most interesting Screenshot:



Errors

Corrupt sample or wrongly selected analyzer.

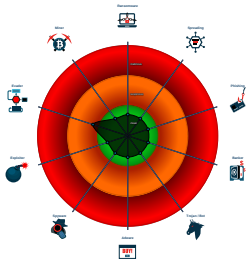
Detection

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Document contains an embedded VB…
- Document contains embedded VBA …

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 152 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

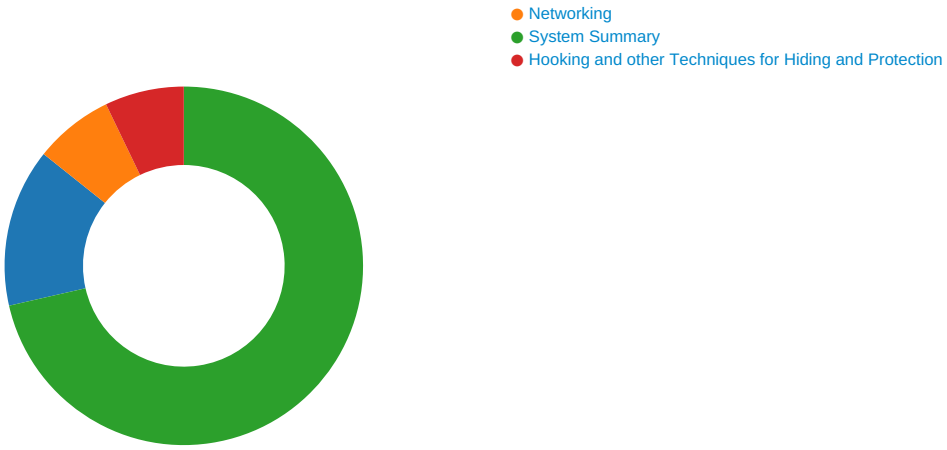
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

● AV Detection



Click to jump to signature section

AV Detection:

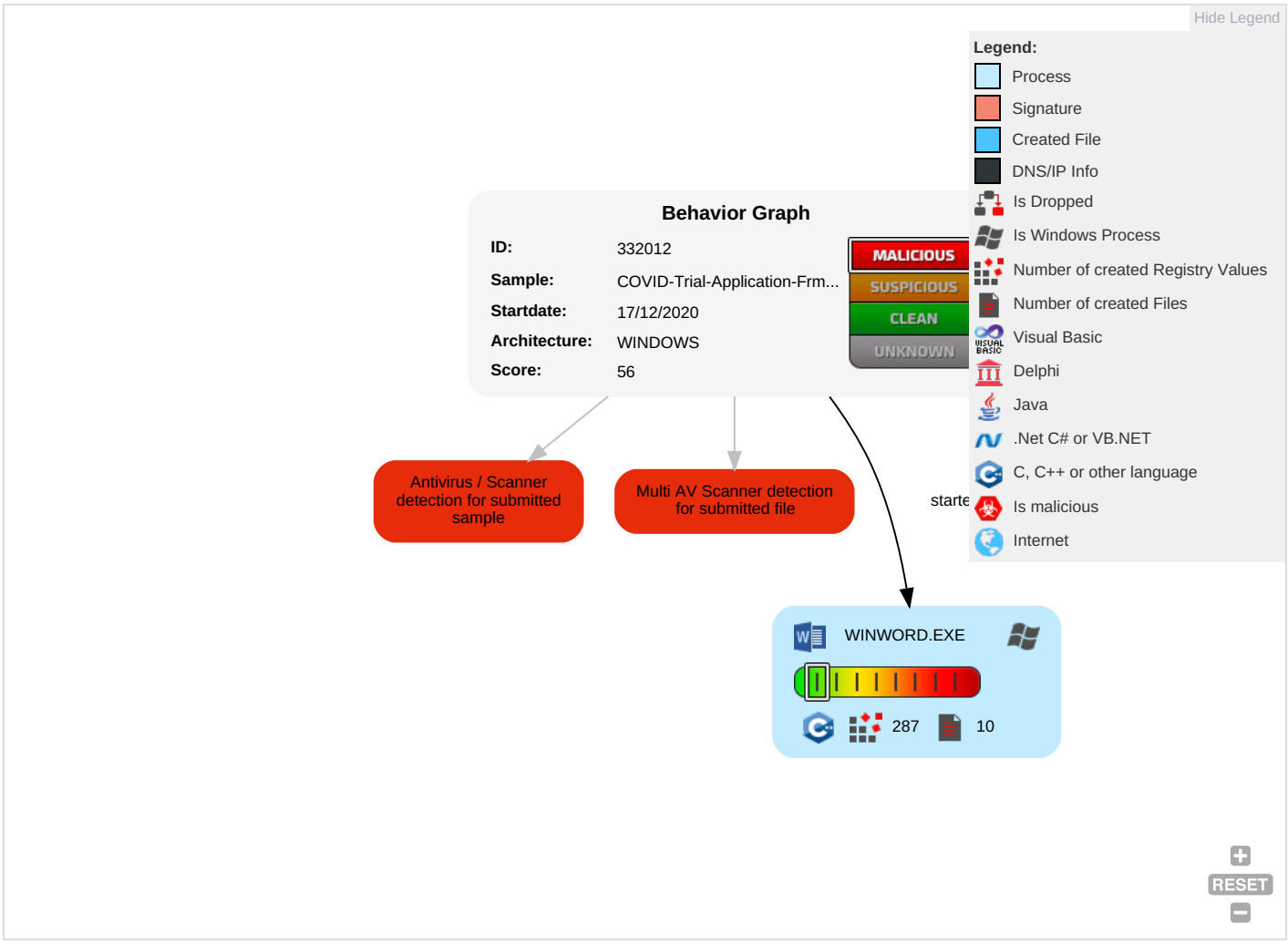
Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

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	Scripting 2	Path Interception	Path Interception	Scripting 2	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	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	System Information Discovery 1	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

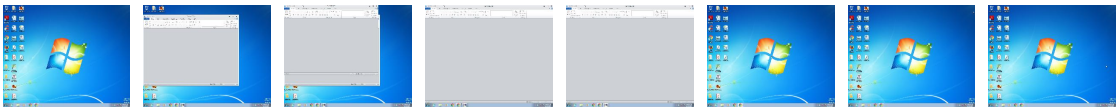
Behavior Graph



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
COVID-Trial-Application-Frm09874x.docx	72%	Virustotal		Browse
COVID-Trial-Application-Frm09874x.docx	58%	Metadefender		Browse
COVID-Trial-Application-Frm09874x.docx	79%	ReversingLabs	Document-Word.Trojan.Powload	
COVID-Trial-Application-Frm09874x.docx	100%	Avira	W97M/Agent.2646611	

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

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	332012
Start date:	17.12.2020
Start time:	23:43:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	COVID-Trial-Application-Frm09874x.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (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:	2
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:	• EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.winDOCX@1/2@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe
Errors:	• Corrupt sample or wrongly selected analyzer.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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\~WRS{73287BFD-FA20-48C4-87C4-17800DB89026}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

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):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2llID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w....z.....w.....x...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Title: Neque., Author: Emilie Mercier, Template: Normal.dotm, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Wed Aug 26 07:08:00 2020, Last Saved Time/Date: Wed Aug 26 07:08:00 2020, Number of Pages: 1, Number of Words: 3, Number of Characters: 20, Security: 0
Entropy (8bit):	6.692763082766669
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:	COVID-Trial-Application-Frm09874x.docx
File size:	225324
MD5:	0343741d7f9a129e1c3af74963343140
SHA1:	5aae176e9f1b9830a498e549aa329b253f40a57f
SHA256:	61e5c441089b95c7879100b308aff42f8e7a059a4f3a5bc861ebd4d25fef58fc
SHA512:	d8088877776f75057d42ab8e03b4c606bf83d7c77cd6cec7b6d641fde97ae9a756dc1a3f2e4a45d5f88bdeadd63c2c045b9a571dd6942b951841615bd5fd3a7a
SSDEEP:	3072:dYy0u8YGgjv+ZvchmkHcl/o1/Vb6////////////////////////2:30uXnWFchmmcl/o1/2zcLwWSeCC
File Content Preview:	.....>.....{.....1...2...4...|.....

File Icon

	
Icon Hash:	e4e6a2a2a4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "COVID-Trial-Application-Frm09874x.docx"

Indicators

Has Summary Info:	True
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:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1252
Title:	Neque.
Subject:	
Author:	Emilie Mercier
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	

Summary	
Revion Number:	1
Total Edit Time:	0
Create Time:	2020-08-26 06:08:00
Last Saved Time:	2020-08-26 06:08:00
Number of Pages:	1
Number of Words:	3
Number of Characters:	20
Creating Application:	Microsoft Office Word
Security:	0

Document Summary	
Document Code Page:	1252
Number of Lines:	1
Number of Paragraphs:	1
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	983040

Streams with VBA

VBA File Name: Her87_tsa69n, Stream Size: -1

General	
Stream Path:	Macros/Her87_tsa69n
VBA File Name:	Her87_tsa69n
Stream Size:	-1
Data ASCII:	
Data Raw:	

VBA Code Keywords

Keyword
Resume
CSng(dKkk))
False
"ds[]a")
VB_Base
"Lnwjsi_gqorknjswkz
VB_Creatable
VB_Exposed
VB_TemplateDerived
Error
Attribute
VB_PredeclaredId
VB_GlobalNameSpace
VB_Name
showwindow
Function
VB_Customizable

VBA Code

VBA File Name: Her87_tsa69n, Stream Size: 14642

General	
Stream Path:	Macros/VBA/Her87_tsa69n
VBA File Name:	Her87_tsa69n
Stream Size:	14642
Data ASCII:	. . . . L . . . . ' . . . . * . . . . N . . . . x . . . . M E . . . .

General	
Data Raw:	01 16 01 00 01 f0 00 00 00 20 05 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 27 05 00 00 af 2a 00 00 00 00 00 00 01 00 00 00 0a 93 1f 4e 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 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

VBA Code Keywords

Keyword
Resume
CSng(dKkk))
False
"ds[]a")
VB_Base
"Lnwjsi_gqorknjswkz
VB_Creatable
VB_Exposed
VB_TemplateDerived
Error
Attribute
VB_PredeclaredId
VB_GlobalNameSpace
VB_Name
showwindow
Function
VB_Customizable

VBA Code

VBA File Name: Y1cfhtdfo8an, Stream Size: 1333

General	
Stream Path:	Macros/VBA/Y1cfhtdfo8an
VBA File Name:	Y1cfhtdfo8an
Stream Size:	1333
Data ASCII:	. . . . V . . . . > . . . . { . . . . < . . . . . J . . . . : Y G . 8 , ... / . , . . . X D . .] . . ` . . . . @ . . . $. S . . . . x . . . . @ . . . $. S . . J . . . . : Y G . 8 , ... M E . . . .
Data Raw:	01 16 01 00 06 00 01 00 00 56 03 00 00 e4 00 00 00 ea 01 00 00 84 03 00 00 92 03 00 00 3e 04 00 00 01 00 00 00 01 00 00 00 0a 93 7b c4 00 00 ff ff a3 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 3c 00 ff ff 00 00 4a f8 80 db 0e 3a 59 47 b7 38 2c f7 e2 11 cc 1f 2f d3 2c 81 f8 05 58 44 bf a2 5d ee f0 60 cf f6 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
Private
VB_Exposed
Attribute
VB_Creatable
VB_Name
Document_open()
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 114

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.2359563651
Base64 Encoded:	True
Data ASCII:	. . . . . F . . . M i c r o s o f t W o r d 9 7 - 2 0 0 3 D o c u m e n t . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 8 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 06 09 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 20 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 57 6f 72 64 20 39 37 2d 32 30 30 33 20 44 6f 63 75 6d 65 6e 74 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 10 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 352

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	352
Entropy:	2.611686106
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . D . . . . . + , . , ... h . . . . . p . . . . . | . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 44 00 00 00 05 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 2c 01 00 00 e8 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 420

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	420
Entropy:	3.2280454647
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . t . . . . . d . . . . . L . . . . . , ... 4 . . . . . < . . . . . D . . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 74 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 64 01 00 00 03 00 00 00 98 00 00 00 04 00 00 00 4c 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 d0 00 00 00 09 00 00 00 dc 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 7035

General	
Stream Path:	1Table
File Type:	data
Stream Size:	7035
Entropy:	5.99786922232
Base64 Encoded:	True
Data ASCII:	. . . . . s . . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	06 06 0f 00 12 00 01 00 73 01 0f 00 07 00 03 00 00 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 136573

General	
Stream Path:	Data
File Type:	data
Stream Size:	136573
Entropy:	7.24646975637

General	
Base64 Encoded:	True
Data ASCII:	} . . . D . d . . . . G 3 . . . . p . . . . A . . . . ? . . . . y . 4 . l . 8 . a . m . 5 . u . h . . . P . i . c . t . u . r . e . . 1 . . . T . y . 4 . l . 8 . a . m . 5 . u . h . . . . . " . . . . R . . . . + i . . . ` . .
Data Raw:	7d 15 02 00 44 00 64 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 bf 47 33 1f fe 01 fe 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 04 f0 a2 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 83 00 0b f0 70 00 00 00 04 41 01 00 00 00 05 c1 16 00 00 00 3f 01 00 00 06 00 bf 01 00 00 10 00 ff 01 00 00

Stream Path: Macros/Her87_tsa69n/\x1CompObj, File Type: data, Stream Size: 97

General	
Stream Path:	Macros/Her87_tsa69n/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	. . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . . 9 . q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/Her87_tsa69n/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 296

General	
Stream Path:	Macros/Her87_tsa69n/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	296
Entropy:	4.62977558511
Base64 Encoded:	True
Data ASCII:	V E R S I O N 5 . 0 0 . . B e g i n { C 6 2 A 6 9 F 0 - 1 6 D C - 1 1 C E - 9 E 9 8 - 0 0 A A 0 0 5 7 4 A 4 F } H e r 8 7 _ t s a 6 9 n . . C a p t i o n = " U s e r F o r m 1 " . . C l i e n t H e i g h t = 3 0 1 5 . . C l i e n t L e f t = 1 2 0 . . C l i e n t T o p = 4 6 5 . . C l i e n t W i d t h = 4 5 6 0 . . S t a r t U p P o s i t i o n = 1 ' C e n t e
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 48 65 72 38 37 5f 74 73 61 36 39 6e 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 31 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20

Stream Path: Macros/Her87_tsa69n/f, File Type: data, Stream Size: 506

General	
Stream Path:	Macros/Her87_tsa69n/f
File Type:	data
Stream Size:	506
Entropy:	4.02860334569
Base64 Encoded:	False
Data ASCII:	. . . . } . . k . . . . 0 . . . . P . . . . j d r 8 4 j j 6 4 f 1 s 4 5 _ b s . . . . , ... L . . . . S d a v a s e q _ z t m b 1 p m . . . . 0 . . . . @ . . . . I h u _ f 5 _ w g n m r 7 8 o _ x y . . . . (. . . . . L . . . . R f n o 8 g m l f 5 u n . . . . 8 . . . .
Data Raw:	00 04 20 00 08 0c 00 0c 09 00 00 00 12 00 00 00 00 7d 00 00 6b 1f 00 00 c6 14 00 00 00 00 00 00 00 00 00 00 00 00 09 00 00 00 cc 01 00 00 00 89 01 00 00 00 30 00 e5 01 00 00 12 00 00 80 01 00 00 00 50 00 00 00 00 00 19 00 5a 6a 64 72 38 34 6a 6a 36 34 66 31 73 34 35 5f 62 73 00 00 00 00 00 00 00 00 00 00 00 00 2c 00 e5 01 00 00 0e 00 00 80 02 00 00 00 4c 00 00 00 01 00 19 00 53 64

Stream Path: Macros/Her87_tsa69n/i05/\x1CompObj, File Type: data, Stream Size: 112

General	
Stream Path:	Macros/Her87_tsa69n/i05/\x1CompObj
File Type:	data
Stream Size:	112
Entropy:	4.6011544911
Base64 Encoded:	False
Data ASCII:	. . . . n ` . . . . . . . . ` . . . . . . M i c r o s o f t F o r m s 2 . 0 F r a m e . . . . . E m b e d d e d O b j e c t . . . . . F o r m s . F r a m e . 1 . . 9 . q . . . .

General	
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 20 18 6e 60 f4 ce 11 9b cd 00 aa 00 60 8e 01 1a 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 72 61 6d 65 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 0e 00 00 00 46 6f 72 6d 73 2e 46 72 61 6d 65 2e 31 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/Her87_tsa69n/i05/f, File Type: data, Stream Size: 44

General	
Stream Path:	Macros/Her87_tsa69n/i05/f
File Type:	data
Stream Size:	44
Entropy:	2.0683698489
Base64 Encoded:	False
Data ASCII:	. . . @ . . . . . } . . . . .
Data Raw:	00 04 20 00 40 0c 02 08 04 80 00 00 03 00 00 00 00 7d 00 00 c4 1d 00 00 d8 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/Her87_tsa69n/i05/o, File Type: empty, Stream Size: 0

General	
Stream Path:	Macros/Her87_tsa69n/i05/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: Macros/Her87_tsa69n/i07/\x1CompObj, File Type: data, Stream Size: 112

General	
Stream Path:	Macros/Her87_tsa69n/i07/\x1CompObj
File Type:	data
Stream Size:	112
Entropy:	4.6011544911
Base64 Encoded:	False
Data ASCII:	. . . . . .n ` . . . . . ` . . . . . M i c r o s o f t F o r m s 2 . 0 F r a m e . . . . . E m b e d d e d O b j e c t . . . . . F o r m s . F r a m e . 1 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 20 18 6e 60 f4 ce 11 9b cd 00 aa 00 60 8e 01 1a 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 72 61 6d 65 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 0e 00 00 00 46 6f 72 6d 73 2e 46 72 61 6d 65 2e 31 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/Her87_tsa69n/i07/f, File Type: data, Stream Size: 44

General	
Stream Path:	Macros/Her87_tsa69n/i07/f
File Type:	data
Stream Size:	44
Entropy:	2.0683698489
Base64 Encoded:	False
Data ASCII:	. . . @ . . . . . } . . . . .
Data Raw:	00 04 20 00 40 0c 02 08 04 80 00 00 03 00 00 00 00 7d 00 00 c4 1d 00 00 d8 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/Her87_tsa69n/i07/o, File Type: empty, Stream Size: 0

General	
Stream Path:	Macros/Her87_tsa69n/i07/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: Macros/Her87_tsa69n/o, File Type: data, Stream Size: 24080

General	
Stream Path:	Macros/Her87_tsa69n/o
File Type:	data
Stream Size:	24080
Entropy:	4.52861483723
Base64 Encoded:	True
Data ASCII:	. . 0 . A . E . . . . . H . , ... { . . . U g z w t m i u _ g d d 1 z g w 5 I . . . . . 5 . . . . T a h o m a . . . . , . A . E . . . . . H . , ... { . . . U t 5 k y u f z j j c 3 1 q a m . . . . 5 . . . . T a h o m a . . . . . A . E . . . . . H . , ... { . . . P . . . . . 5 . . . . T a h o m a 6 . . . , . A . E . . . . . H . , ... { . . . T I 0 2
Data Raw:	00 02 30 00 41 01 45 80 00 00 00 00 1b 48 80 2c 03 01 02 00 11 00 00 80 ec 09 00 00 7b 02 00 00 55 67 7a 77 74 6d 69 75 5f 67 64 64 31 7a 67 77 35 49 2e 0f 00 02 18 00 35 00 00 00 06 00 00 80 a5 00 00 00 00 02 00 00 54 61 68 6f 6d 61 00 00 00 02 2c 00 41 01 45 80 00 00 00 00 1b 48 80 2c 03 01 02 00 10 00 00 80 ec 09 00 00 7b 02 00 00 55 74 35 6b 79 75 66 7a 6a 6a 63 33 31 71 61 6d

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 510

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	510
Entropy:	5.41307394677
Base64 Encoded:	True
Data ASCII:	I D = " { 0 3 7 6 D 7 E 2 - 8 1 E 5 - 4 D 0 2 - A 8 E 9 - 3 E 2 0 E A 5 A 7 2 C 4 } " . . D o c u m e n t = Y 1 c f h t d f o 8 a n / & H 0 0 0 0 0 0 0 0 . . P a c k a g e = { A C 9 F 2 F 9 0 - E 8 7 7 - 1 1 C E - 9 F 6 8 - 0 0 A A 0 0 5 7 4 A 4 F } . . B a s e C l a s s = H e r 8 7 _ t s a 6 9 n . . E x e N a m e 3 2 = " J t j c n g c 1 j 8 c j 7 x q s e " . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 7
Data Raw:	49 44 3d 22 7b 30 33 37 36 44 37 45 32 2d 38 31 45 35 2d 34 44 30 32 2d 41 38 45 39 2d 33 45 32 30 45 41 35 41 37 32 43 34 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 59 31 63 66 68 74 64 66 6f 38 61 6e 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 50 61 63 6b 61 67 65 3d 7b 41 43 39 46 32 46 39 30 2d 45 38 37 37 2d 31 31 43 45 2d 39 46 36 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 0d 0a 42

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 80

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	80
Entropy:	3.47192809489
Base64 Encoded:	False
Data ASCII:	Y 1 c f h t d f o 8 a n . Y . 1 . c . f . h . t . d . f . o . 8 . a . n . . . H e r 8 7 _ t s a 6 9 n . H . e . r . 8 . 7 . _ . t . s . a . 6 . 9 . n . . . . .
Data Raw:	59 31 63 66 68 74 64 66 6f 38 61 6e 00 59 00 31 00 63 00 66 00 68 00 74 00 64 00 66 00 6f 00 38 00 61 00 6e 00 00 00 48 65 72 38 37 5f 74 73 61 36 39 6e 00 48 00 65 00 72 00 38 00 37 00 5f 00 74 00 73 00 61 00 36 00 39 00 6e 00 00 00 00 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 14330

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	14330
Entropy:	5.40893568443
Base64 Encoded:	True
Data ASCII:	. a . . . . . * . \ \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \ \ . P . R . O . G . R . A . ~ . 2 . \ \ . C . O . M . M . O . N . ~ . 1 . \ \ . M . I . C . R . O . S . ~ . 1 . \ \ . V . B . A . \ \ . V . B . A . 7 . . . 1 . \ \ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c .
Data Raw:	cc 61 a3 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 06 00 02 00 fe 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: Macros/VBA/__SRP_0, File Type: data, Stream Size: 1534

General	
Stream Path:	Macros/VBA/__SRP_0
File Type:	data
Stream Size:	1534

General	
Entropy:	4.52531312411
Base64 Encoded:	False
Data ASCII:	. K * . . . . * \\ C N o r m a l r U . . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ h . . . . 1 . . . . v . . E E . z . . . S . 9 . . . . e . . . . y . . . . Q . . . .
Data Raw:	93 4b 2a a3 01 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 01 00 09 00 00 00 2a 5c 43 4e 6f 72 6d 61 6c 72 55 80 01 00 00 80 00 00 00 80 00 00 00 80 00 00 00 04 00 00 7e 05 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00

Stream Path: Macros/VBA/__SRP_1, File Type: data, Stream Size: 106

General	
Stream Path:	Macros/VBA/__SRP_1
File Type:	data
Stream Size:	106
Entropy:	2.10825159249
Base64 Encoded:	False
Data ASCII:	r U . . . . ~ } . . . . p . . . .
Data Raw:	72 55 80 00 00 00 80 00 00 00 80 00 00 00 80 00 00 00 01 00 00 7e 7d 00 00 7f 00 00 00 00 0a 00 00 00 09 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 09 00 00 00 00 00 03 00 ff ff ff 03 00 00 09 11 03 00 00 00 00 00 00 09 08 00 00 00 00 00 00 08 00 00 00 00 00 01 00 70 00 00 7f 00 00 00 00

Stream Path: Macros/VBA/__SRP_2, File Type: data, Stream Size: 304

General	
Stream Path:	Macros/VBA/__SRP_2
File Type:	data
Stream Size:	304
Entropy:	2.29666421023
Base64 Encoded:	False
Data ASCII:	r U . . . . 0 . . . . i . . . . 4 . . . . a . . . . 1 . . . . ` . . . . 0 . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 1e 00 00 00 09 00 00 00 00 00 00 00 09 00 00 00 00 00 03 00 30 00 00 00 00 00 00 00 01 00 01 00 00 00 00 00 01 00 01 00 00 00 01 00 91 07 00 00 00 00 00 00 b9 07 00 00 00 00 00 00 e1 07 00 00 00 00 00 00 09 00 00 00 01 00 02 00 69 07 00 00 00 00 00 00 08 00 0d 00 34 00 00 00 09 08 00 00 00 00 00 00 61 00 00 00 00 00

Stream Path: Macros/VBA/__SRP_3, File Type: data, Stream Size: 103

General	
Stream Path:	Macros/VBA/__SRP_3
File Type:	data
Stream Size:	103
Entropy:	2.16020154321
Base64 Encoded:	False
Data ASCII:	r U . . . . @ . . . . . $ . . . . ` . . . . n . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff 00 00 00 00 40 00 00 00 04 00 24 00 01 01 00 00 00 00 02 00 00 00 04 60 00 00 ec 06 1c 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 1e 00 00 00 00 00 00 6e 00 00 7f 00 00 00 00

Stream Path: Macros/VBA/dir, File Type: MIPSEB MIPS-III ECOFF executable not stripped - version 72.3, Stream Size: 836

General	
Stream Path:	Macros/VBA/dir
File Type:	MIPSEB MIPS-III ECOFF executable not stripped - version 72.3
Stream Size:	836
Entropy:	6.4798951851
Base64 Encoded:	True

General	
Data ASCII:	. @ . . . . . 0 * . . . . p . . H . . . . . d . . . . N o r m a l r r Q . (. . @ . . . . . = ... l . . . . y 7 3 a . . . . J . < . . . . . r s t d . o l e > . . s . t . . d . o . l . e P . . . h . % ^ . . * . \\ G { 0 0 0 2 0 . 4 3 0 - . . . . C . . . . 0 0 4 6 } # . 2 . 0 # 0 # C : . \\ W i n d o w s . \\ S y s W O W 6 4 . 4 \\ . e 2 . t l b . # O L E A u t . o m a t i o n . ` . . . . E N o r m a l . . E N . C r . m . a Q . F . . . . . * , \\ C . . . . V . m . .
Data Raw:	01 40 b3 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 07 00 1c 00 4e 6f 72 6d 61 6c 72 72 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 14 08 06 12 09 02 12 80 79 37 33 61 0d 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30

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

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	4096
Entropy:	1.23871150966
Base64 Encoded:	False
Data ASCII:	. . . . [. . . . . b j b j . . . . . p a ! \\ p ! \\ . . . . . s . . . . . s . . . . . s . . . . . s . . . . . s . . . . .
Data Raw:	ec a5 c1 00 5b e0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 17 08 00 00 0e 00 62 6a 62 6a 12 0b 12 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 04 16 00 2e 0e 00 00 70 61 21 5c 70 61 21 5c 17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 152 Parent PID: 584

General

Start time:	23:43:33
Start date:	17/12/2020
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:	0x13f520000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly