ID: 558779
Sample Name: XSG2363662.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:30:47
Date: 24/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

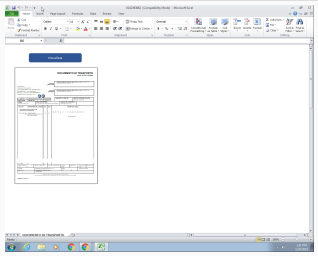
Windows Analysis Report

XSG2363662.xls

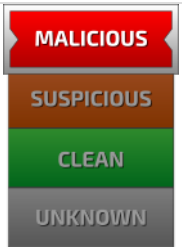
Overview

General Information

Sample Name:	XSG2363662.xls
Analysis ID:	558779
MD5:	0a18e47e743c2a..
SHA1:	434030db9b84e3.
SHA256:	6b3407cfd0ef9a6..
Tags:	BRT gozi isfb ursnif xls
Infos:	SIGMA



Detection



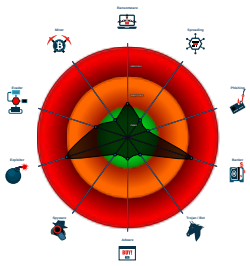
Ursnif Dropper

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Detected Italy targeted Ursnif dropp…
- Document contains an embedded V…
- Sigma detected: Suspicious Remote…
- Document contains embedded VBA…
- Document misses a certain OLE str…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2796 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary

Sigma detected: Suspicious Remote Thread Created

Jbx Signature Overview

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

E-Banking Fraud

Detected Italy targeted Ursnif dropper document

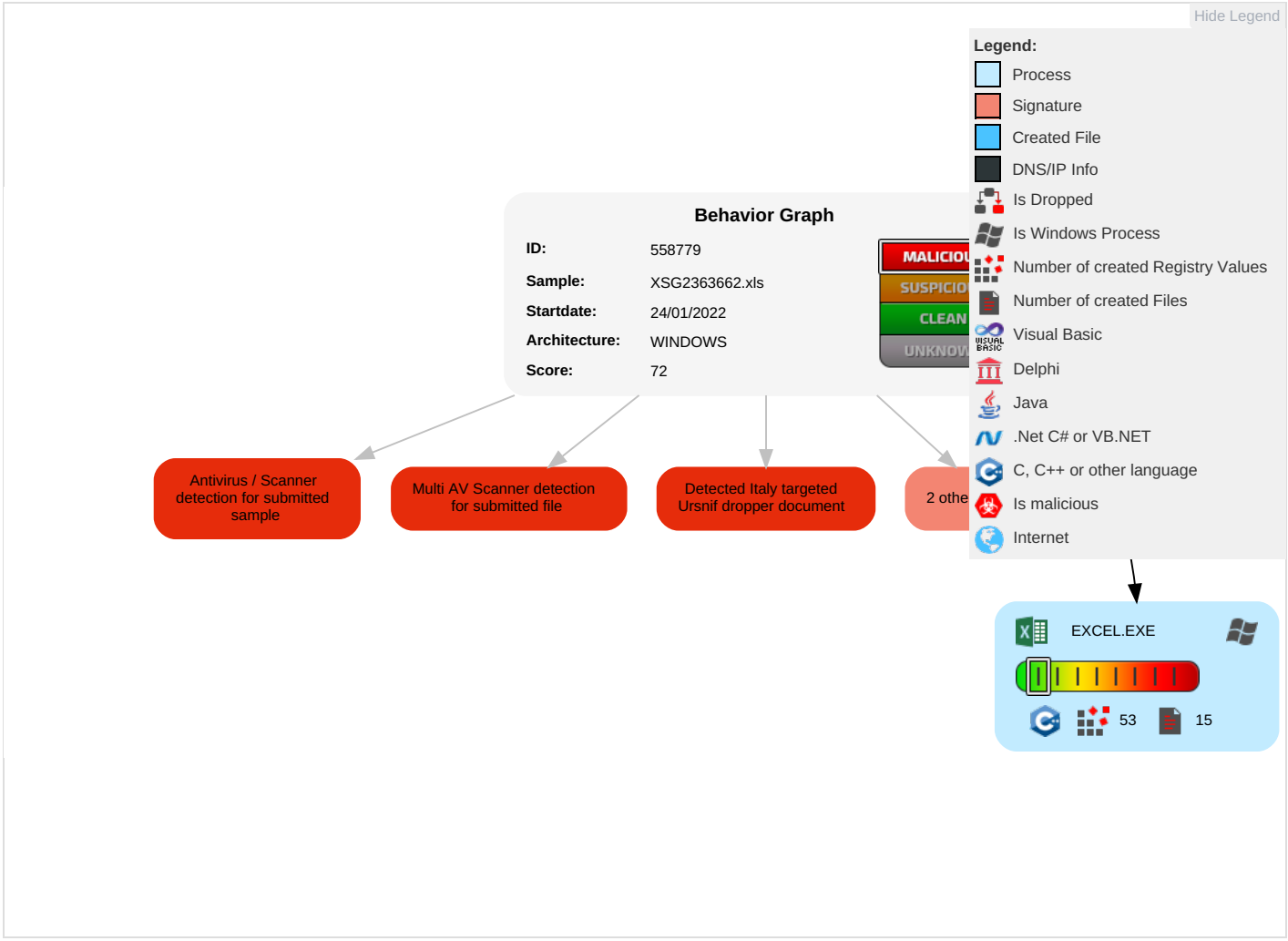
System Summary

Document contains an embedded VBA macro with suspicious strings

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Scripting	Path Interception	Path Interception	1 1 Scripting	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	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

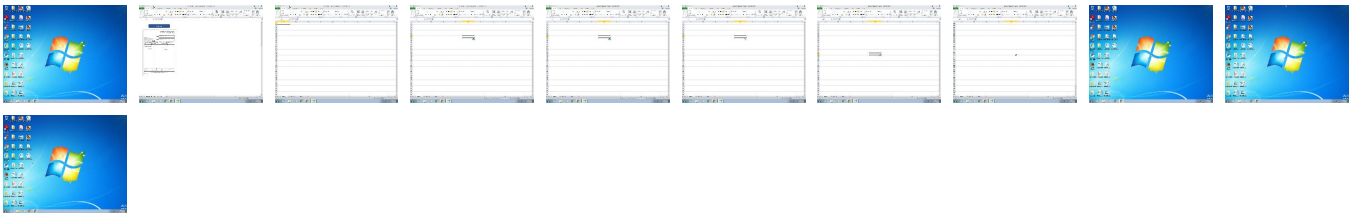
Behavior Graph

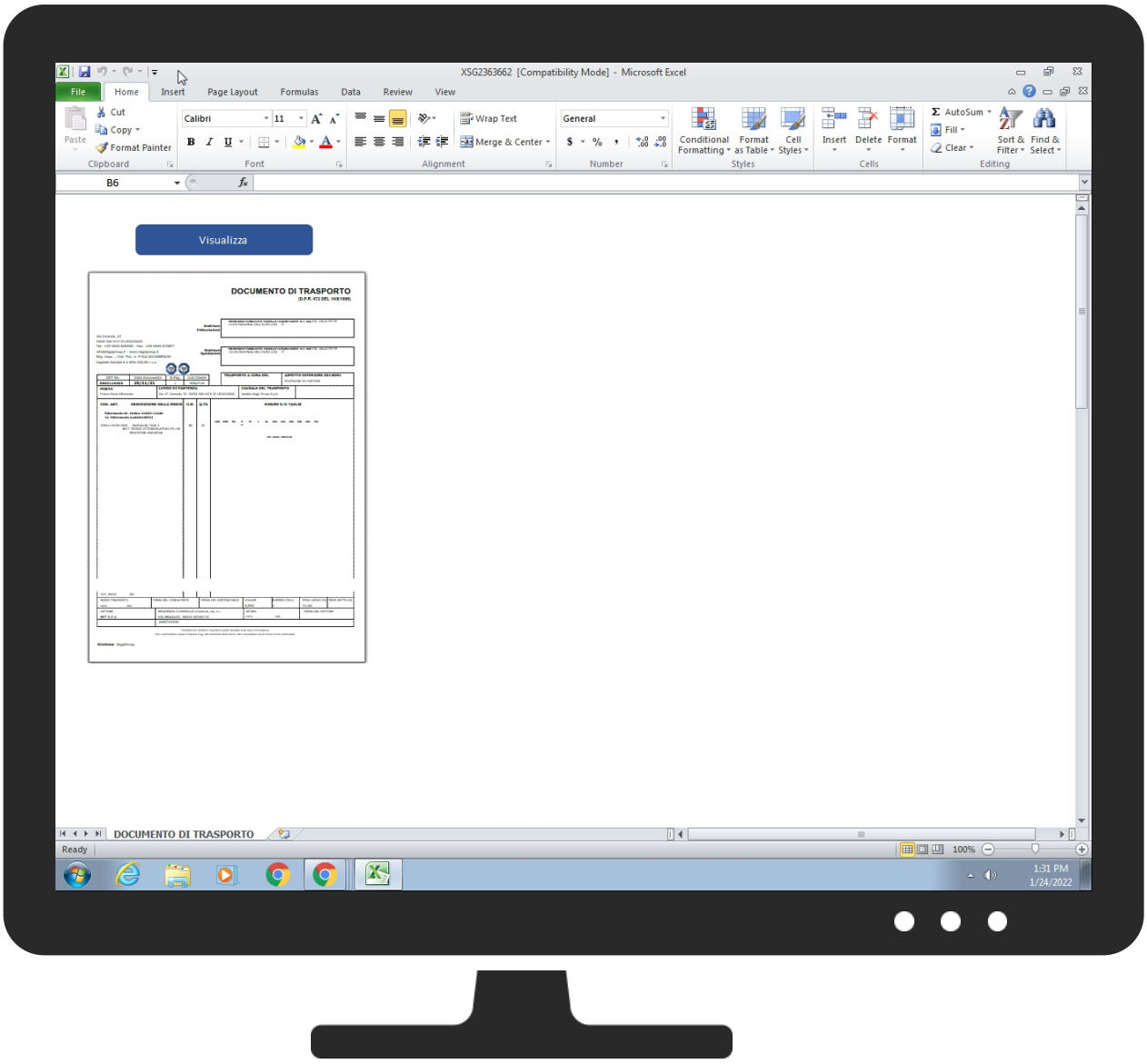


Screenshots

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
XSG2363662.xls	10%	Virustotal		Browse
XSG2363662.xls	14%	ReversingLabs	Script-Macro.Trojan.Heuristic	
XSG2363662.xls	100%	Avira	HEUR/Macro.Downloader.MRAJM.Gen	

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:	34.0.0 Boulder Opal
Analysis ID:	558779
Start date:	24.01.2022
Start time:	13:30:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	XSG2363662.xls
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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.bank.expl.winXLS@1/4@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active Picture Object • Active AutoShape Object • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe

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\Temp\3977.tmp

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsalTlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB39E
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DF1716BD010027B375.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	32768

Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BB7DF04E1B0A2570657527A7E108AE23
SHA1:	5188431849B4613152FD7BDBA6A3FF0A4FD6424B
SHA-256:	C35020473AED1B4642CD726CAD727B63FFF2824AD68CEDD7FFB73C7CBD890479
SHA-512:	768007E06B0CD9E62D50F458B9435C6DDA0A6D272F0B15550F97C478394B743331C3A9C9236E09AB5B9CB3B423B2320A5D66EB3C7068DB9EA37891CA40E4701
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF67575D7F5A6EBB68.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.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\Local\Temp\~DF85705E9879F41F79.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.8512955148344692
Encrypted:	false
SSDEEP:	384:t//coCkERoz4GoMmV8oN9XHtNjcuwNRaT9E:ub31kW1NNjCNRaTC
MD5:	8494ED2F1A80D7BDE64639EF733E6DBD
SHA1:	0FA6ED2833098C4D5F047AF1929CC8E17F4CE3F3
SHA-256:	7A5253BF9AD0149AE1C0D2E116164F05A880757127FD0087F3A923A24411BBBF
SHA-512:	EE4A562FFC2017E630CFFA37D8D3D30994953EA1B1016DA5B34FC920FC2E462FF701718F13DA5AF5735C88A5FFC23B9D7AE2B7726F714A122C9F39089B78BF0D
Malicious:	false
Reputation:	low
Preview:	....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: VETTORE; BRT S .P .A., Name of Creating Application: Microsoft Excel, Create Time/Date: Mon Jan 24 11:15:40 2022, Last Saved Time/Date: Mon Jan 24 11:15:43 2022, Security: 0
Entropy (8bit):	5.511085804898523
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%

File name:	XSG2363662.xls
File size:	50176
MD5:	0a18e47e743c2a3bdb26333764d4d19c
SHA1:	434030db9b84e3832e5cc1019137205aa1c9de6f
SHA256:	6b3407cfd0ef9a6664e61733b8a838b9cd1d05e084a36a8eff0dddb0e21d34c4
SHA512:	d94effd3ac78e9a722d9cfbaf0612a7cf19e68b99a870f58869f4d0b6dbcbcd5b7a6df22c471161a178d8e7d713e5a31534a1c22830740bc83d139f62300246d
SSDEEP:	1536:bsQlYkEIbSkKBEqEXPgsRZmbaoFhZhR0cixIHm09s4av3b+mMC9EM:bhlYkEIuPm3fNRZmbaoFhZhR0cixIHmw
File Content Preview:	.....>.....:.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "XSG2363662.xls"

Indicators

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

Summary

Code Page:	1252
Author:	VETTORE; BRT S .P .A.
Last Saved By:	
Create Time:	2022-01-24 11:15:40.064000
Last Saved Time:	2022-01-24 11:15:43
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams with VBA

VBA File Name: Foglio1, Stream Size: 1000

General

Stream Path:	_VBA_PROJECT_CUR/VBA/Foglio1
VBA File Name:	Foglio1
Stream Size:	1000

Data ASCII:	. . . . . 5 . . . . . B z v . . . . . # . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 01 f0 00 00 00 da 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff e1 02 00 00 35 03 00 00 00 00 00 00 01 00 00 00 42 7a 76 de 00 00 ff ff 23 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 00 00 00 00 00 00

VBA Code

VBA File Name: Questa_cartella_di_lavoro, Stream Size: 5189	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Questa_cartella_di_lavoro
VBA File Name:	Questa_cartella_di_lavoro
Stream Size:	5189
Data ASCII:	. . . . . @ . . . N . . . r . . . . . B z Z . . . . . # . . . . . p . . . . .] . . J l . ' . . . 4 . . . . . F . . . . . n . s K . . . l . ^ C . X . . . . . x . . . . n . s K . . . l . ^ C . X . . . . .] . . J l . ' . . . 4 . . . . . M . . . . .
Data Raw:	01 16 03 00 03 00 01 00 00 12 0a 00 00 e4 00 00 00 10 02 00 00 40 0a 00 00 4e 0a 00 00 72 10 00 00 00 00 00 00 01 00 00 00 42 7a 5a b4 00 00 ff ff 23 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 70 00 ff ff 00 00 b2 d9 ee 5d 8d e7 4a 49 b3 27 d6 8f ce 34 8c b8 19 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 00 46 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

Streams	
Stream Path: \x1CompObj, File Type: data, Stream Size: 118	
General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	118
Entropy:	4.32915524493
Base64 Encoded:	True
Data ASCII:	. . . . . F * . . . (F o g l i o d i l a v o r o d i M i c r o s o f t E x c e l 2 0 0 3 . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 8 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 2a 00 00 00 28 46 6f 67 6c 69 6f 20 64 69 20 6c 61 76 6f 72 6f 20 64 69 20 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 20 32 30 30 33 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 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: 268	
General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	268
Entropy:	3.12865032743
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . P . . . . . X . . . . . d . . . . . l . . . . . t . . . . . | . . . . . D O C U M E N T O D I T R A S P O R T O . . . . . F o g l i d i l a v o r
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 dc 00 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 b2 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 220	
General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	220
Entropy:	3.64969681825
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . T . . . . . l . . . . . x . . . . . M i c r o s o f t E x c e l . @ . . . . Z ? . . . . . @ . . . . Y . . . . . V E T T O R E ; B R T S . P . A . . . .

General	
Data Raw:	fe ff 00 00 0a 00 02 00 00 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 ac 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 8c 00 00 00 08 00 00 00 48 00 00 00 12 00 00 00 54 00 00 00 0c 00 00 00 6c 00 00 00 0d 00 00 00 78 00 00 00 13 00 00 00 84 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 28420

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	28420
Entropy:	6.49399582728
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . B . . . . . a . . . . = ... Q u e s t a _ c a r t e l l a _ d i _ l a v o r o . . . . = ... C
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 454

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	454
Entropy:	5.41897951506
Base64 Encoded:	True
Data ASCII:	I D = " { 2 F 2 C 6 4 B F - 5 E 3 3 - 4 F 7 E - 9 6 2 B - D 1 1 3 A A 1 9 7 8 8 A } " . . D o c u m e n t = Q u e s t a _ c a r t e l l a _ d i _ l a v o r o / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = F o g l i o 1 / & H 0 0 0 0 0 0 0 0 . . N a m e = " V B A 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 = " 4 9 4 B B D 3 B C 1 3 B C 1 3 B C 1 3 B C 1 " . . D P B = " E C E E 1 8 4 1 1 8 E 5 1 9 E 5 1 9 E 5 " . . G C = " 8 F
Data Raw:	49 44 3d 22 7b 32 46 32 43 36 34 42 46 2d 35 45 33 33 2d 34 46 37 45 2d 39 36 32 42 2d 44 31 31 33 41 41 31 39 37 38 38 41 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 51 75 65 73 74 61 5f 63 61 72 74 65 6c 6c 61 5f 64 69 5f 6c 61 76 6f 72 6f 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 46 6f 67 6c 69 6f 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 56

Stream Path: _VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 104

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECTwm
File Type:	data
Stream Size:	104
Entropy:	3.33133492199
Base64 Encoded:	False
Data ASCII:	Q u e s t a _ c a r t e l l a _ d i _ l a v o r o . Q . u . e . s . t . a . _ . c . a . r . t . e . l . l . a . _ . d . i . _ . l . a . v . o . r . o . . . F o g l i o 1 . F . o . g . l . i . o . 1 . . . . .
Data Raw:	51 75 65 73 74 61 5f 63 61 72 74 65 6c 6c 61 5f 64 69 5f 6c 61 76 6f 72 6f 00 51 00 75 00 65 00 73 00 74 00 61 00 5f 00 63 00 61 00 72 00 74 00 65 00 6c 00 6c 00 61 00 5f 00 64 00 69 00 5f 00 6c 00 61 00 76 00 6f 00 72 00 6f 00 00 00 46 6f 67 6c 69 6f 31 00 46 00 6f 00 67 00 6c 00 69 00 6f 00 31 00 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: data, Stream Size: 3138

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3138
Entropy:	4.52314617839
Base64 Encoded:	False
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 . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b5 00 00 03 00 ff 10 04 00 00 09 04 00 00 e4 04 03 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 20 01 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 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: _VBA_PROJECT_CUR/VBA/__SRP_0, File Type: data, Stream Size: 2014

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_0
File Type:	data
Stream Size:	2014
Entropy:	3.42400406956

General	
Base64 Encoded:	False
Data ASCII:	. K * . . . . . r U . . . . . @ . . . . . @ . . . . . @ . . . . . ~ . . . . . ~ . . . . . ~ . . . . . ~ . . . . . ~ Z . . . . . " . . . . . Q . . . . . ! . . . . s . E . . y . . . . .
Data Raw:	93 4b 2a b5 03 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 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 00 00 72 55 c0 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 06 00 00 00 00 00 00 7e 0a 00 00 00 00 00 00 7e 02 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_1, File Type: data, Stream Size: 252	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_1
File Type:	data
Stream Size:	252
Entropy:	1.8302935157
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . @ . . . . . ~ z . . . . . q . . . . . A . . . . . e d . . . . . s . . . . . R . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 02 00 00 00 00 00 00 7e 7a 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 12 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 11 00 00 00 00 00 00 00 03 00 ff ff ff ff ff ff ff 06 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_2, File Type: data, Stream Size: 1601	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_2
File Type:	data
Stream Size:	1601
Entropy:	2.20269951636
Base64 Encoded:	False
Data ASCII:	r U . . . . . @ . . . . . @ . . . . . 8 . . . . . P . . . . . A . . . . . 7 . ` . . . q . . . . .
Data Raw:	72 55 c0 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01 00 00 00 01 00 d1 03 00 00 00 00 00 00 00 00 00 00 11 08 00 00 00 00 00 00 00 00 00 41 08

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_3, File Type: data, Stream Size: 926	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_3
File Type:	data
Stream Size:	926
Entropy:	2.47413380681
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . x . . . . . @ . . . . . ` . . . . . P . @ . . . . . ` . . . . . O . @ . . . . . ` . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 40 00 e1 01 00 00 00 00 00 00 00 00 02 00 00 00 03 60 04 01 d9 08 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 562	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/dir
File Type:	data
Stream Size:	562
Entropy:	6.26356984503
Base64 Encoded:	True
Data ASCII:	. . . . . 0 . J . . . . H . . H . . . . . H . . . d . . . . . V B A P r @ o j e c t . . . . T . @ . . . . . = . . . + . r . . . . . c . . . . J < . . . . . 9 s t d o l . e . . s . t . d . . o . l . e . . . . 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 t e m 3 2 \\ . . e 2 . t l b # O . L E A u t o m . a t i o n . 0 . . . E O f f i c . E O . . f . . i . c . E . . . . . E 2 D F 8 D
Data Raw:	01 2e b2 80 01 00 04 00 00 00 03 00 30 aa 4a 02 90 02 00 48 02 02 48 09 00 c0 12 14 06 48 03 00 01 64 e4 04 04 04 00 0a 00 84 56 42 41 50 72 40 6f 6a 65 63 74 05 00 1a 00 54 00 40 02 0a 06 02 0a 3d 02 0a 07 2b 02 72 01 14 08 06 12 09 02 12 0f 08 a0 e7 63 02 00 0c 02 4a 3c 02 0a 04 16 00 01 39 73 74 64 6f 6c 04 65 3e 02 19 73 00 74 00 64 00 00 6f 00 6c 00 65 00 0d 14 00 68 00 25 5e

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 2796, Parent PID: 596

General

Start time:	13:31:15
Start date:	24/01/2022
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13ffc0000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
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\3977.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14015DABF	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\3977.tmp	success or wait	1	1401C090C	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~s~	success or wait	1	6E630648	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.png	C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~s~	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htmss	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image005.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image005.pngss	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image006.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image006.pngss	success or wait	1	6E630648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	6E630648	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E60A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E60A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E60A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\3426D	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\34B04	success or wait	1	6E630648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	5q-	binary	35 71 2D 00 EC 0A 00 00 02 00 00 00 00 00 00 00 40 00 00 00 01 00 00 00 1E 00 00 00 16 00 00 00 78 00 73 00 67 00 32 00 33 00 36 00 33 00 36 00 36 00 32 00 2E 00 78 00 6C 00 73 00 00 00 78 00 73 00 67 00 32 00 33 00 36 00 33 00 36 00 36 00 32 00 00 00	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6422942404.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3024948866.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9655434068.xlsx	success or wait	1	6E630648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1287572840.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8182259827.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6750529025.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6109303877.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9925478147.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5491630718.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9659692161.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0653671941.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1237160943.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0450125302.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6329227256.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6183211589.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7457734050.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1141274626.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9329238007.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3643399760.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3476888679.xlsx	success or wait	1	6E630648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\3426D	3426D	binary	04 00 00 00 EC 0A 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 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 01 00 00 00 01 00 00 00 AA 41 00 C7 69 11 D8 01 6D 42 03 00 6D 42 03 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6422942404.xlsx	success or wait	1	6E630648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3024948866.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9655434068.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1287572840.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8182259827.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6750529025.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6109303877.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9925478147.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5491630718.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9659692161.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0653671941.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1237160943.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0450125302.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6329227256.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6183211589.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7457734050.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1141274626.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9329238007.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3643399760.xlsx	success or wait	1	6E630648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3476888679.xlsx	success or wait	1	6E630648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\34B04	34B04	binary	04 00 00 00 EC 0A 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 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 01 00 00 00 01 00 00 00 AA 41 00 C7 69 11 D8 01 04 4B 03 00 04 4B 03 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E630648	unknown

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

Disassembly

No disassembly