ID: 736957
Sample Name: xls.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:44:29
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

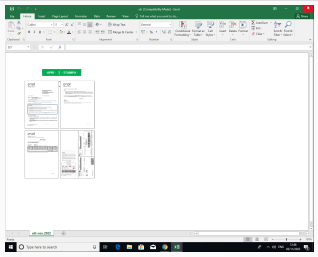
Windows Analysis Report

xls.xls

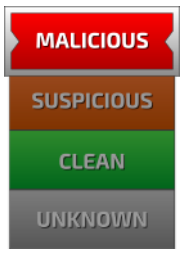
Overview

General Information

Sample Name:	xls.xls
Analysis ID:	736957
MD5:	109d15a7d33e67.
SHA1:	c6660d40673400..
SHA256:	822d2e533e0537.
Tags:	xls
Infos:	HTTP



Detection

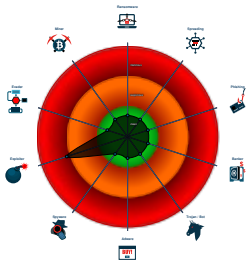


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Document contains an embedded V…
- Document contains an embedded V…
- Document contains an embedded V…
- Machine Learning detection for sam…
- Document contains an embedded V…
- Document contains embedded VBA…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 5752 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary

Document contains an embedded VBA with functions possibly related to ADO stream file operations

Document contains an embedded VBA macro which may execute processes

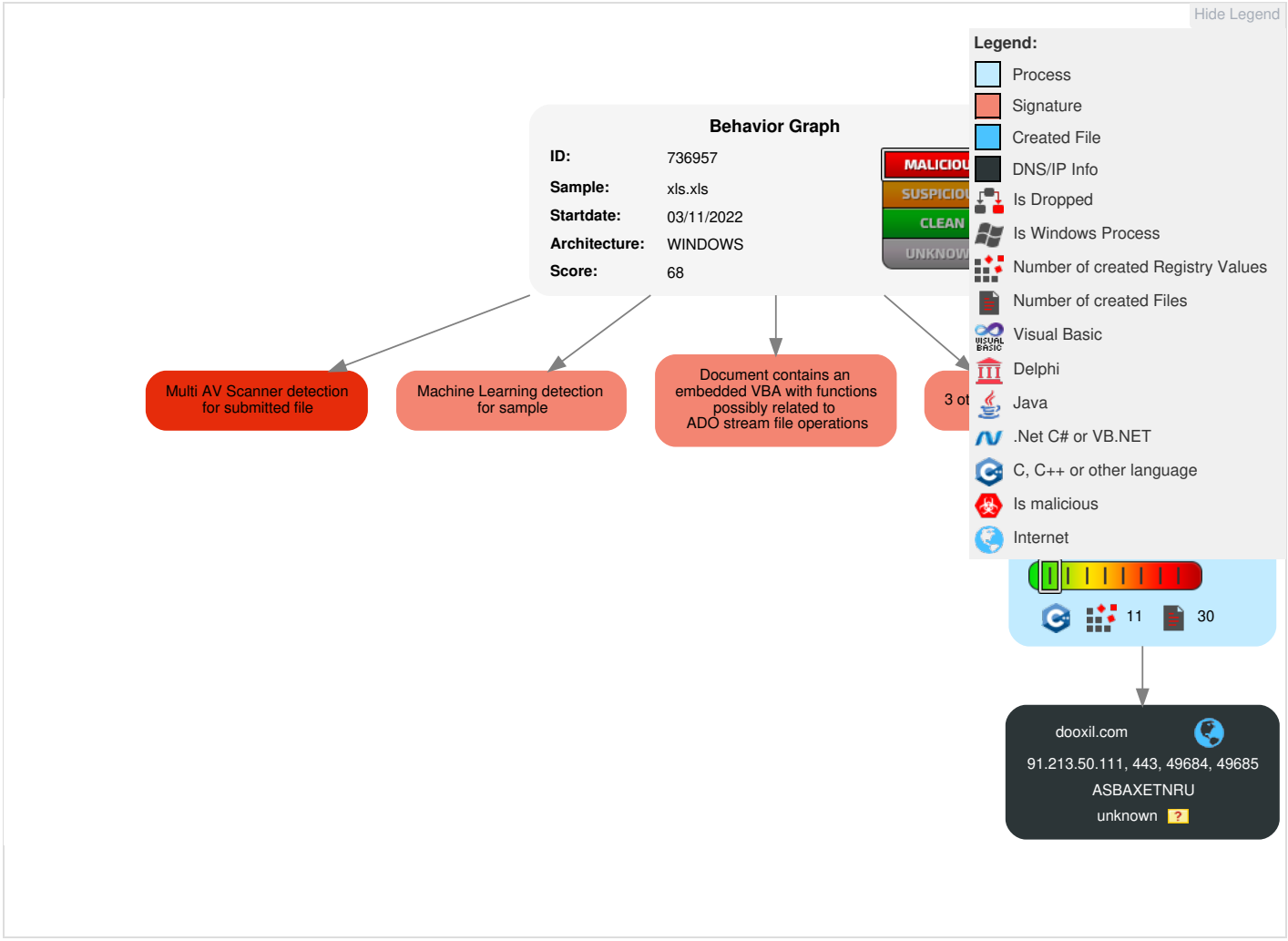
Document contains an embedded VBA macro with suspicious strings

Document contains an embedded VBA with functions possibly related to HTTP operations

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	4 1 Scripting	Path Interception	Path Interception	4 1 Scripting	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	3 Exploitation for Client Execution	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	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

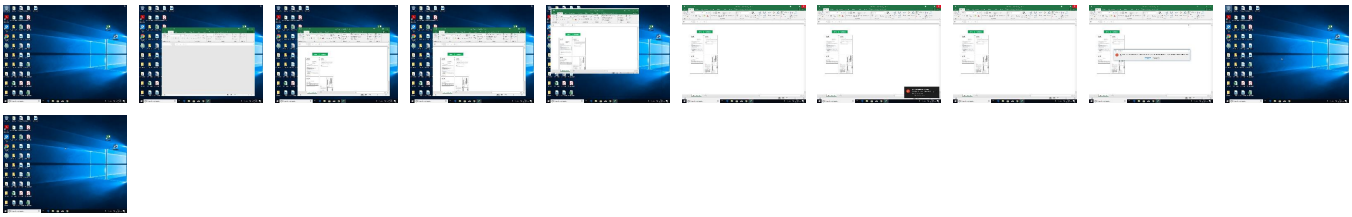
Behavior Graph

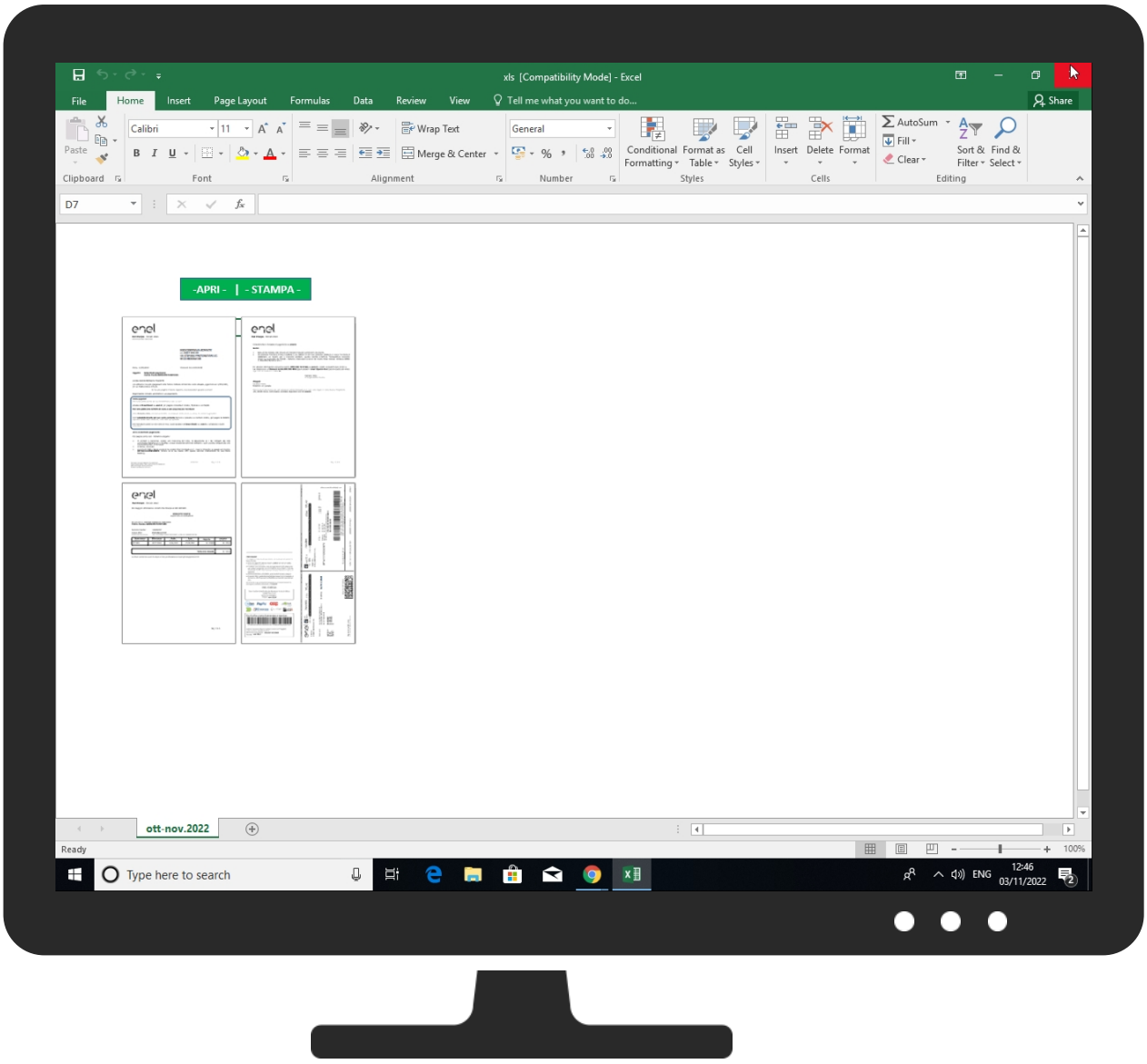


Screenshots

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
xls.xls	17%	ReversingLabs	Win32.Trojan.Valyria	
xls.xls	40%	Virustotal		Browse
xls.xls	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

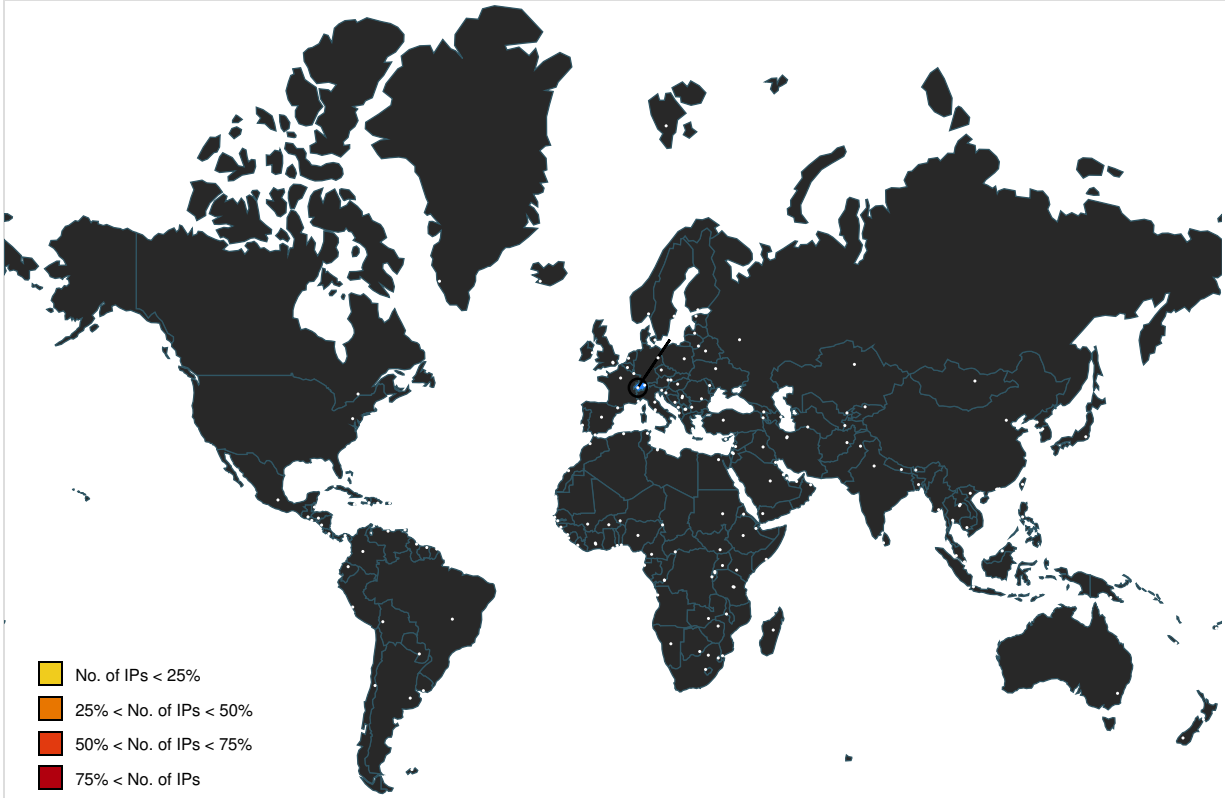
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dooxil.com	91.213.50.111	true	false		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.213.50.111	dooxil.com	unknown		49392	ASBAXETNRU	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736957
Start date and time:	2022-11-03 12:44:29 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	xls.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	8
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.expl.winXLS@1/0@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xls • Changed system and user locale, location and keyboard layout to Italian - Italy • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active Picture Object • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): ocos-office365-s2s.msedge.net, client-office365-tas.msedge.net, ctldl.windowsupdate.com, config.edge.skype.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtReadVirtualMemory 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

No created / dropped files found

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: Enel SpA, Name of Creating Application: Microsoft Excel, Create Time/Date: Thu Nov 3 08:32:50 2022, Last Saved Time/Date: Thu Nov 3 08:32:57 2022, Security: 0
Entropy (8bit):	5.342866000055418
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	xls.xls
File size:	69120
MD5:	109d15a7d33e671ded911d97bc4a15ab
SHA1:	c6660d40673400505c70af85dfddc735fa50a39f
SHA256:	822d2e533e0537f92fa3ddcbd8cb2a0d7c33ba2ada626e1cae4ecf466ac61e9b
SHA512:	1789d8a5381b24d58150eefb1748b7fa7c5c0782acf53796b517f258d178d6175d4e78717fd4a64c206fd0ee9d8b9bd29444ccc1ef35a337b8ad50548146ce30
SSDEEP:	1536:JcblYkElbSkKBEqEXPgsRZmbaoFhZhR0cixIHm0YtjY+N81LobstcIUvcGJ/uW:2blYkEIuPm3fNRZmbaoFhZhR0cixIHmZ
TLSH:	E1630969775AC987D6552F364CE6D7E97336BC40AE9B83073104B73E6F7A6C0C902206
File Content Preview:	.....>.....<.....|.....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "xls.xls"

Indicators

Has Summary Info:	
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:	False
Flash Objects Count:	0
Contains VBA Macros:	True

Summary

Code Page:	1252
Author:	
Last Saved By:	
Create Time:	2022-11-03 08:32:50.891000
Last Saved Time:	2022-11-03 08:32:57
Creating Application:	
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.cls, Stream Size: 13465	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Foglio1
VBA File Name:	Foglio1.cls
Stream Size:	13465
Data ASCII:	. . . . . # . . . . . # . . # . . - . . . . . \\ . . # . . . . . p . . . : b r . t L . H . ! . . . . . F . . . . . = * . p . F L Q 5 0 9 . . . . . x . . . . = * . p . F L Q 5 0 9 : b r . t L . H . ! . . . . . M E . . . . . P . . . . . [L . . . . S . . . . . S . . . . > ' . . . . . L . . . . .
Data Raw:	01 16 03 00 06 00 01 00 00 12 23 00 00 e4 00 00 00 88 02 00 00 b2 23 00 00 c0 23 00 00 8c 2d 00 00 00 00 00 00 01 00 00 00 16 b5 2e 5c 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 93 3a 62 72 0b ae 74 4c b8 05 48 1e 97 21 02 8f 20 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

VBA File Name: Questa_cartella_di_lavoro.cls, Stream Size: 1203	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Questa_cartella_di_lavoro
VBA File Name:	Questa_cartella_di_lavoro.cls
Stream Size:	1203
Data ASCII:	. . . . . Z . . . . . r . . # . . . . . p . . . F j . ~ D] i . . F . . . . . F . . . . . ' 9 . $. D . x . . . . . x . . . . ' 9 . $. D .] x . F j . ~ D] i . . F . . . . M E . . . . . (. . . . . S L . . . . S . . . . . S . . . . 6 " . . . . . . 0 . { . 0 . 0 . 0 . 2 . 0 . 8 . 1 . 9 . - . 0 . 0 . 0
Data Raw:	01 16 03 00 06 00 01 00 00 5a 03 00 00 e4 00 00 00 10 02 00 00 88 03 00 00 96 03 00 00 ea 03 00 00 00 00 00 00 01 00 00 00 16 b5 86 72 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 46 eb f7 a2 6a 1d 7e 44 96 5d 69 02 99 1e cd 46 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: 117	
General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	117
Entropy:	4.295052233063858
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 29 00 00 00 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: 256	
General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	256
Entropy:	2.843729876697485
Base64 Encoded:	True
Data ASCII:	. . . . . + , 0 . . . . . P . . . . . X . . . . . d . . . . . l . . . . . t . . . . . | . . . . . o t t - n o v . 2 0 2 2 . . . . . F o g l i d i l a v o r o . . . . .

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 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 d0 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 a5 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 208

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	208
Entropy:	3.4571641941803213
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 . @ . . . . E ^ . @ . . . B ^ . . . . E n e l S p A . . . .
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 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a0 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: 28945

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	28945
Entropy:	6.62615417319298
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 . # 8 . . . . X . @ . .
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

Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 521

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	521
Entropy:	5.248358244801769
Base64 Encoded:	True
Data ASCII:	I D = " { 0 0 0 0 0 0 0 0 - 0 0 0 0 - 0 0 0 0 - 0 0 0 0 - 0 0 0 0 0 0 0 0 0 0 0 0 } " . . 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 . . H e l p F i l e = " " . . 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 = " C C C E 6 0 F E 6 0 8 6 6 4 8 6 6 4 8 2 6 8 8 2 6 8 " . . D P B = " 5 0 5 2 F C E 3 1 9 E 3
Data Raw:	49 44 3d 22 7b 30 30 30 30 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 30 30 30 30 30 30 30 30 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 48 65 6c 70 46 69 6c

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:	3.331334921988963
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: 3570

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3570
Entropy:	4.762300417602462

General	
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 . . . D .
Data Raw:	cc 61 b2 00 00 03 00 ff 00 20 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: 4673	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_0
File Type:	data
Stream Size:	4673
Entropy:	3.4972369321145735
Base64 Encoded:	False
Data ASCII:	K * . . . . r U . . . . @ . . . . @ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . . ~ . . . . ~ . . . . ~ . . . .
Data Raw:	93 4b 2a b2 03 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 02 00 01 00 00 00 00 00 01 00 00 00 01 00 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 00 00 72 55 c0 03 00 00 00 00 00 00 80 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 06 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_1, File Type: data, Stream Size: 452	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_1
File Type:	data
Stream Size:	452
Entropy:	2.541028075676919
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . @ . . . . ~ . . . . ~ v . . . . q . . . . 0 . . . . t r a g u a r d o . . . . p i t t o r e . . . .
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 02 00 00 00 00 00 00 7e 76 00 00 00 00 00 00 7f 00 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 00 00 00 00 11 00 00 00 00 00 00 00 00 00 05 00 11 00 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_2, File Type: data, Stream Size: 828	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_2
File Type:	data
Stream Size:	828
Entropy:	2.4574353505314255
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . x . . . . . P . . . . ` . . . . . . . 1 . . . . . . . . . . . . . . . . . . . P . . . . . . . . . . . . . . . . ` . . . . a . . . . P . @ . . . . ` . . . . . . . . . . . . . O . P . . . . . . . . . . . . . . . . ` . . . . O . O . X . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 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 03 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 50 00 e1 01 00 00 00 00 00 00 00 00 03 00 00 00 03 60 08 01 e9 04 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_3, File Type: data, Stream Size: 6472	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_3
File Type:	data
Stream Size:	6472
Entropy:	3.743290714587534
Base64 Encoded:	False
Data ASCII:	r U . . . . @ . . . . @ . . . . 8 . . . . 0 . . . A . . . . A . . . . 4 . . . . ! . . . . a . . . . ! . . . .
Data Raw:	72 55 80 01 00 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 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 02 00 d0 04 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 30 00 00 00 41 0c 00 00 00 00 00 00 00 00 00 00 c1 0d 00 00 00 00 00 00 00 00 00 00 41 0f 00 00 00 00 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_4, File Type: data, Stream Size: 680

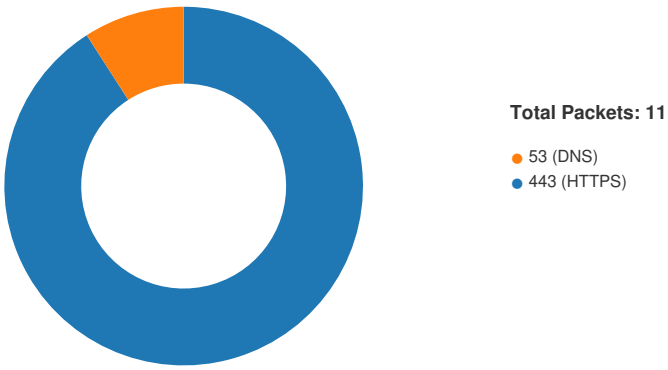
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_4
File Type:	data
Stream Size:	680
Entropy:	1.3016690799486477
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . 8 . . . . . A . . . . . 7 . ` . . . q . . . . . D . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 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 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 05 00 b0 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 11 08 00 00 00 00 00 00 00 00 00 41 08

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_5, File Type: data, Stream Size: 106	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_5
File Type:	data
Stream Size:	106
Entropy:	1.3591119461716878
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . x . . . . . b . . . . .
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 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 04 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 00 00 00 00 00 00 62 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 558	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/dir
File Type:	data
Stream Size:	558
Entropy:	6.191417516649333
Base64 Encoded:	True
Data ASCII:	. * . . . . . 0 * . . . . p . . H . . . . d . . . . . V B A P r o j e c t . . 4 . . @ . . j . . . = ... r . . . . . c e . . . . J < . . . . . r 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 . ` . . E O f f D i c E O . f . i . c E . . E . 2 D F 8 D 0 4 C . - 5 B F A - 1 0 1 B - B D E 5 E A A C 4 . 2 E
Data Raw:	01 2a b2 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 8b f1 63 65 04 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:46:23.901690960 CET	49684	443	192.168.2.5	91.213.50.111

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:46:23.901755095 CET	443	49684	91.213.50.111	192.168.2.5
Nov 3, 2022 12:46:23.901866913 CET	49684	443	192.168.2.5	91.213.50.111
Nov 3, 2022 12:46:23.909301996 CET	49684	443	192.168.2.5	91.213.50.111
Nov 3, 2022 12:46:23.909348011 CET	443	49684	91.213.50.111	192.168.2.5
Nov 3, 2022 12:48:34.267613888 CET	443	49684	91.213.50.111	192.168.2.5
Nov 3, 2022 12:48:34.271982908 CET	49685	443	192.168.2.5	91.213.50.111
Nov 3, 2022 12:48:34.272059917 CET	443	49685	91.213.50.111	192.168.2.5
Nov 3, 2022 12:48:34.272176981 CET	49685	443	192.168.2.5	91.213.50.111
Nov 3, 2022 12:48:34.272639036 CET	49685	443	192.168.2.5	91.213.50.111
Nov 3, 2022 12:48:34.272672892 CET	443	49685	91.213.50.111	192.168.2.5
Nov 3, 2022 12:50:45.339247942 CET	443	49685	91.213.50.111	192.168.2.5
Nov 3, 2022 12:50:45.343519926 CET	49689	443	192.168.2.5	91.213.50.111
Nov 3, 2022 12:50:45.343581915 CET	443	49689	91.213.50.111	192.168.2.5
Nov 3, 2022 12:50:45.343719006 CET	49689	443	192.168.2.5	91.213.50.111
Nov 3, 2022 12:50:45.343904972 CET	49689	443	192.168.2.5	91.213.50.111
Nov 3, 2022 12:50:45.343949080 CET	443	49689	91.213.50.111	192.168.2.5
Nov 3, 2022 12:50:45.344654083 CET	49689	443	192.168.2.5	91.213.50.111

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:46:23.721085072 CET	60136	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:46:23.889734983 CET	53	60136	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 3, 2022 12:46:23.721085072 CET	192.168.2.5	8.8.8.8	0xa44c	Standard query (0)	dooxil.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 3, 2022 12:46:23.889734983 CET	8.8.8.8	192.168.2.5	0xa44c	No error (0)	dooxil.com		91.213.50.111	A (IP address)	IN (0x0001)	false

Statistics

No statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 5752, Parent PID: 788

General

Target ID:	0
Start time:	12:45:29
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding
Imagebase:	0xa50000
File size:	27110184 bytes

MD5 hash:	5D6638F2C8F8571C593999C58866007E
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\~DFF923C22ADA0AC914.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	675892AB	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	675DD539	unknown
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	675DD539	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	675DD539	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	675DD539	unknown
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	675DD539	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	675DD539	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	675DD539	unknown
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	675DD539	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	675DD539	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	675DD539	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	675DD539	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	675DD539	unknown

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6FA29601	WriteFile
unknown	2	44	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6FA29601	WriteFile
unknown	46	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6FA29601	WriteFile
unknown	50	36	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6FA29601	WriteFile
unknown	86	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6FA29601	WriteFile
unknown	90	38	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	6FA29601	WriteFile
unknown	128	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	6FA29601	WriteFile
unknown	176	20	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	6FA29601	WriteFile
unknown	196	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	6FA29601	WriteFile
unknown	200	68	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	6FA29601	WriteFile
unknown	814	20	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	6FA29601	WriteFile
unknown	834	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	6	6FA29601	WriteFile
unknown	838	68	75 6e 6b 6e 6f 77 6e	unknown	success or wait	8	6FA29601	WriteFile
unknown	1082	158	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	6FA29601	WriteFile
unknown	1240	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	11	6FA29601	WriteFile
unknown	1286	68	75 6e 6b 6e 6f 77 6e	unknown	success or wait	11	6FA29601	WriteFile

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\Office\Common\ExdCache	success or wait	1	AC20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	AC211C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	675C8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	675C8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	675C8A84	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	AC213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	AC213B	RegSetValueExW

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

Disassembly

No disassembly