

JoeSandbox Cloud BASIC



ID: 558645

Sample Name:

sample20220124-01.xls

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 10:57:24

Date: 24/01/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report sample20220124-01.xls	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Overview	4
Sigma Overview	4
Jbx Signature Overview	4
AV Detection	5
E-Banking Fraud	5
System Summary	5
Mitre Att&ck Matrix	5
Behavior Graph	5
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	8
Domains and IPs	8
Contacted Domains	8
World Map of Contacted IPs	8
General Information	8
Warnings	8
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASNs	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
C:\Users\user\AppData\Local\Temp\41FF.tmp	9
C:\Users\user\AppData\Local\Temp\~DF12FD691A8C519DA7.TMP	9
C:\Users\user\AppData\Local\Temp\~DF53CCF8CC4483A0FB.TMP	10
C:\Users\user\AppData\Local\Temp\~DFA1A8704CE37CB6FE.TMP	10
Static File Info	10
General	10
File Icon	11
Static OLE Info	11
General	11
OLE File "sample20220124-01.xls"	11
Indicators	11
Summary	11
Document Summary	11
Streams with VBA	11
VBA File Name: Foglio1, Stream Size: 992	11
General	11
VBA Code	12
VBA File Name: Questa_cartella_di_lavoro, Stream Size: 5151	12
General	12
VBA Code	12
Streams	12
Stream Path: \x1CompObj, File Type: data, Stream Size: 118	12
General	12
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 268	12
General	12
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 212	12
General	12
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 28393	13
General	13
Stream Path: _VBA_PROJECT_CUR\PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 452	13
General	13
Stream Path: _VBA_PROJECT_CUR\PROJECTwm, File Type: data, Stream Size: 104	13
General	13
Stream Path: _VBA_PROJECT_CUR\VBA\ _VBA_PROJECT, File Type: data, Stream Size: 3023	13
General	13
Stream Path: _VBA_PROJECT_CUR\VBA\ _SRP_0, File Type: data, Stream Size: 2012	13
General	13
Stream Path: _VBA_PROJECT_CUR\VBA\ _SRP_1, File Type: data, Stream Size: 252	14
General	14
Stream Path: _VBA_PROJECT_CUR\VBA\ _SRP_2, File Type: data, Stream Size: 2641	14
General	14
Stream Path: _VBA_PROJECT_CUR\VBA\ _SRP_3, File Type: data, Stream Size: 926	14
General	14
Stream Path: _VBA_PROJECT_CUR\VBA\dir, File Type: data, Stream Size: 562	14
General	14
Network Behavior	14

Statistics	15
System Behavior	15
Analysis Process: EXCEL.EXEPID: 1892, Parent PID: 596	15
General	15
File Activities	15
File Created	15
File Deleted	15
File Moved	15
Registry Activities	16
Key Created	16
Key Value Created	16
Disassembly	20

Windows Analysis Report

sample20220124-01.xls

Overview

General Information

Sample Name:

sample20220124-01.xls

Analysis ID:

558645

MD5:

4e8ec74a93b831..

SHA1:

330af52281a3a9..

SHA256:

e68fcd845683be..

Tags:

BRT

gozi

isfb

ursnif

xls

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Ursnif Dropper

Score:

68

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Antivirus / Scanner detection for sub...

Multi AV Scanner detection for subm...

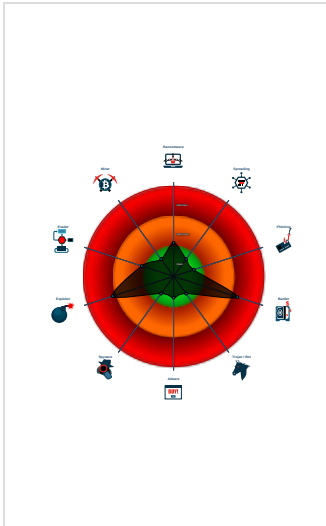
Detected Italy targeted Ursnif dropp...

Document contains an embedded V...

Document contains embedded VBA...

Document misses a certain OLE str...

Classification



Process Tree

System is w7x64

EXCELEXE (PID: 1892 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)

cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

E-Banking Fraud



Detected Italy targeted Ursnif dropper document

System Summary

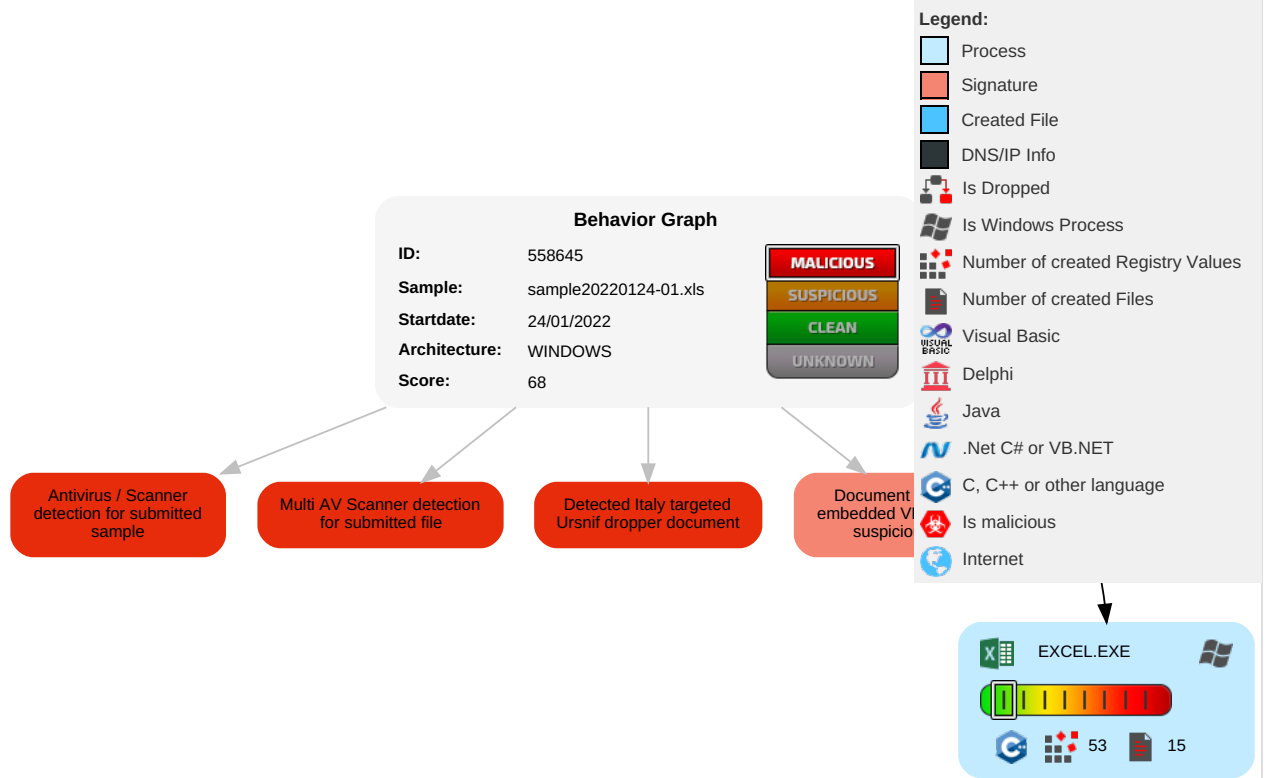


Document contains an embedded VBA macro with suspicious strings

Mitre Att&ck Matrix

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

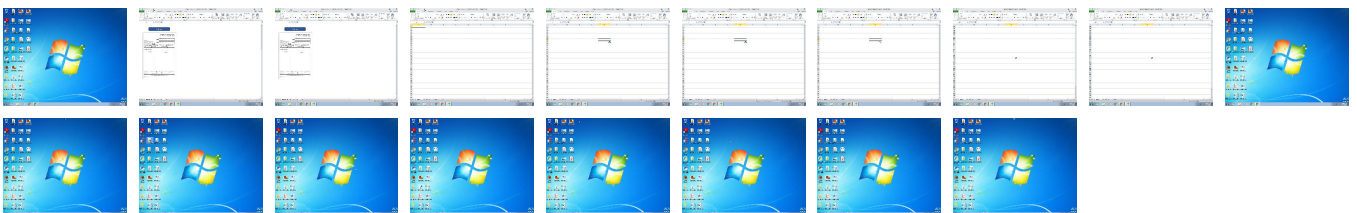
Behavior Graph

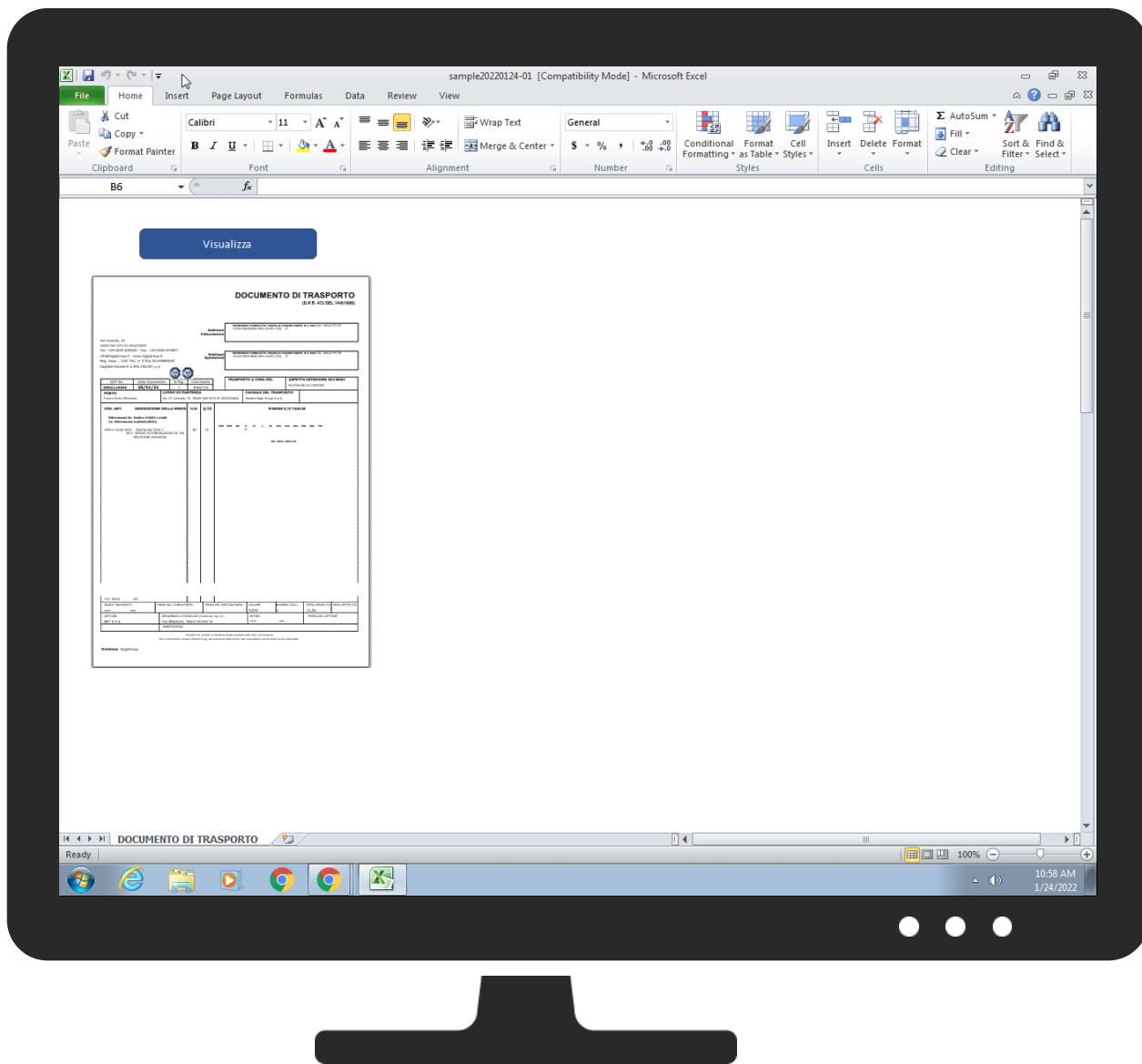


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
sample20220124-01.xls	11%	Virustotal		Browse
sample20220124-01.xls	12%	ReversingLabs	Script-Macro.Downloader.Heuristic	
sample20220124-01.xls	100%	Avira	HEUR/Macro.Downloader.MRAJM.Gen	

Dropped Files

⊘ No Antivirus matches

Unpacked PE Files

⊘ No Antivirus matches

Domains

⊘ No Antivirus matches

URLs

🚫 No Antivirus matches

Domains and IPs

Contacted Domains

🚫 No contacted domains info

World Map of Contacted IPs

🚫 No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	558645
Start date:	24.01.2022
Start time:	10:57:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sample20220124-01.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	3
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.bank.expl.winXLS@1/4@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active Picture Object • Active AutoShape Object • Scroll down • Close Viewer

Warnings

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

Simulations

Behavior and APIs

 No simulations

Joe Sandbox View / Context

IPs

 No context

Domains

 No context

ASNs

 No context

JA3 Fingerprints

 No context

Dropped Files

 No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\41FF.tmp

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsaTILPtl2N81HRQjIORGt7RQ//W1XR9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB39E
Malicious:	false
Reputation:	high, very likely benign file
Preview:	>.....

C:\Users\user\AppData\Local\Temp~-DF12FD691A8C519DA7.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	73728

Entropy (8bit):	1.8483782394368125
Encrypted:	false
SSDEEP:	384:qo/jrfCQRtQMm58jR92nbtiiHaTNRaZ9E:qQTJthfUnRiHKNRaZC
MD5:	38550BD20211F44AEAD2B61E44C206C1
SHA1:	D829F35503C1D84B9C8A277BD06B1A65EFBD708F
SHA-256:	AF2B719D8E6ECC6F3C46778F65C1129F34A95CD7AD8128198AED426C711FFC33
SHA-512:	5A1C8B74B326D507A6AB79102528AE0F4CAB6A8A04788E25F5D045C3785414B6B65D778C767393CCA66006E17A3DAA19564722E6C291A785F2CD5F4B1320A8A
Malicious:	false
Reputation:	low
Preview:	

C:\Users\user\AppData\Local\Temp\~DF53CCF8CC4483A0FB.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	

C:\Users\user\AppData\Local\Temp\~DFA1A8704CE37CB6FE.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BB7DF04E1B0A2570657527A7E108AE23
SHA1:	5188431849B4613152FD7BDBA6A3FF0A4FD6424B
SHA-256:	C35020473AED1B4642CD726CAD727B63FFF2824AD68CEDD7FFB73C7CBD890479
SHA-512:	768007E06B0CD9E62D50F458B9435C6DDA0A6D272F0B15550F97C478394B743331C3A9C9236E09AB5B9CB3B423B2320A5D66EB3C7068DB9EA37891CA40E4701
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	

Static File Info	
General	
File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: VETTORE BRT S.P.A., Create Time/Date: Mon Jan 24 08:04:38 2022, Last Saved Time/Date: Mon Jan 24 08:04:41 2022, Security: 0, Comments: DATA ORA
Entropy (8bit):	5.4276709427017735
TrID:	- Microsoft Excel sheet (30009/1) 78.94% - Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	sample20220124-01.xls

File size:	51200
MD5:	4e8ec74a93b831a92a1b016722e79365
SHA1:	330af52281a3a9ae4836062f98f77fe5f8a834e4
SHA256:	e68fcd845683be392885de766f158a1c6b00cea57bdd68b5ff44d54e62400e1f
SHA512:	68dfa7849da02bd108d78a14686a7c7eded8e45206208fd8afda9886262b12dfafda475c0ed1dfef46dd48c41f9e5048364d158a0a82279d8fedaf226cd5aa22
SSDEEP:	1536:fsQlYkElbSkKBEqEXPgsRZmbaoFhZhR0cixlHm0hs4avxDdmsicY:fhlYkEluPm3fNRZmbaoFhZhR0cixlHmg
File Content Preview:	>.....;.....

File Icon	
	
Icon Hash:	e4eea286a4b4bcb4

Static OLE Info	
General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "sample20220124-01.xls"	
Indicators	
Has Summary Info:	True
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Code Page:	1252
Author:	VETTORE BRT S.P.A.
Comments:	DATA ORA
Last Saved By:	
Create Time:	2022-01-24 08:04:38.805000
Last Saved Time:	2022-01-24 08:04:41
Security:	0

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

Streams with VBA	
VBA File Name: Foglio1, Stream Size: 992	
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Foglio1
VBA File Name:	Foglio1
Stream Size:	992
Data ASCII:	 - B z v # x M E

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 268	
General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	268
Entropy:	3.12865032743
Base64 Encoded:	False
Data ASCII:	+,...0.....P.....X.....d.....l.....t.....DOCUMENTO DI TRASPORTOFogli di lavor
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 dc 00 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 b2 00 00 00

Page 12 of 21

General	
Data Raw:	93 4b 2a b5 03 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 00 00 00 00 01 00 02 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 72 55 c0 00 00 00 00 00 05 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 7e 02 00 00 00 00 00 7e 02 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/_SRP_1, File Type: data, Stream Size: 252

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_SRP_1
File Type:	data
Stream Size:	252
Entropy:	1.8302935157
Base64 Encoded:	False
Data ASCII:	r U @ @ @ @ ~ z q A e d s R
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 02 00 00 00 00 00 7e 7a 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 12 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 11 00 00 00 00 00 00 00 03 00 ff ff ff ff ff ff 06 00 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/_SRP_2, File Type: data, Stream Size: 2641

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_SRP_2
File Type:	data
Stream Size:	2641
Entropy:	1.97225478766
Base64 Encoded:	False
Data ASCII:	r U @ @ 8 A 7 q
Data Raw:	72 55 c0 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 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 11 00 00 00 00 00 00 00 03 00 d0 00 00 00 00 00 00 00 00 00 0d 00 0d 00 00 00 00 01 00 01 00 00 00 01 d1 03 00 00 00 00 00 00 00 00 11 08 00 00 00 00 00 00 00 00 00 41 08

Stream Path: _VBA_PROJECT_CUR/VBA/_SRP_3, File Type: data, Stream Size: 926

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_SRP_3
File Type:	data
Stream Size:	926
Entropy:	2.47413380681
Base64 Encoded:	False
Data ASCII:	r U @ @ @ x @ P . @ ` O . @
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 11 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 78 00 00 00 08 00 40 00 e1 01 00 00 00 00 00 00 00 02 00 00 00 03 60 04 01 d9 08 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 562

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/dir
File Type:	data
Stream Size:	562
Entropy:	6.2614646746
Base64 Encoded:	True
Data ASCII:	 0 . J H H d V B A P r @ o j e c t T . @ = + . r 7 c J < 9 s t d o l . e > s . t . d l . e h . % ^ . . . * \ G . { 0 0 0 2 0 4 3 . 0 - C 0 0 4 6 } # 2 . . 0 # 0 # C : \ W . i n d o w s \ S . y s t e m 3 2 \ . . e 2 . t l b # O . L E A u t o m . a t i o n . 0 . . . E O f f i c . E O . f . i . c . E E 2 D F 8 D
Data Raw:	01 2e b2 80 01 00 04 00 00 00 03 00 30 aa 4a 02 90 02 00 48 02 02 48 09 00 c0 12 14 06 48 03 00 01 64 e4 04 04 04 00 0a 00 84 56 42 41 50 72 40 6f 6a 65 63 74 05 00 1a 00 54 00 40 02 0a 06 02 0a 3d 02 0a 07 2b 02 72 01 14 08 06 12 09 02 12 37 08 a0 e3 63 0d 00 0c 02 4a 3c 02 0a 04 16 00 01 39 73 74 64 6f 6c 04 65 3e 02 19 73 00 74 00 64 00 00 6f 00 6c 00 65 00 0d 14 00 68 00 25 5e

Network Behavior

 No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 1892, Parent PID: 596

General

Start time:	10:58:16
Start date:	24/01/2022
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13f4a0000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\41FF.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	13F63DABF	GetTempFile NameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	6E550648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	6E550648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	6E550648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	6E550648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	6E550648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~	success or wait	1	6E550648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml~	success or wait	1	6E550648	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	6E550648	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	6E550648	unknown
C:\Users\user\AppData\Local\Temp\41FF.tmp	success or wait	1	13F6A090C	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	6E550648	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	6E550648	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	6E550648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~s~	success or wait	1	6E550648	unknown
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	6E550648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.png	C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~s~	success or wait	1	6E550648	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Templmgs_files\filelist.xml	C:\Users\user\AppData\Local\Templmgs_files\filelist.xml--s~	success or wait	1	6E550648	unknown
C:\Users\user\AppData\Local\Templmgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Templmgs_files\stylesheet.css..	success or wait	1	6E550648	unknown
C:\Users\user\AppData\Local\Templmgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Templmgs_files\tabstrip.htmss	success or wait	1	6E550648	unknown
C:\Users\user\AppData\Local\Templmgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Templmgs_files\sheet001.htmss	success or wait	1	6E550648	unknown
C:\Users\user\AppData\Local\Templmgs_files\sheet002.ht_	C:\Users\user\AppData\Local\Templmgs_files\sheet002.htmss	success or wait	1	6E550648	unknown
C:\Users\user\AppData\Local\Templmgs_files\image005.pn_	C:\Users\user\AppData\Local\Templmgs_files\image005.pngss	success or wait	1	6E550648	unknown
C:\Users\user\AppData\Local\Templmgs_files\image006.pn_	C:\Users\user\AppData\Local\Templmgs_files\image006.pngss	success or wait	1	6E550648	unknown
C:\Users\user\AppData\Local\Templmgs_files\filelist.xml_	C:\Users\user\AppData\Local\Templmgs_files\filelist.xmlss	success or wait	1	6E550648	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\VB	success or wait	1	6E52A5E3	RegCreateKeyExA	
HKEY_CURRENT_USER\Software\Microsoft\VB\7.0	success or wait	1	6E52A5E3	RegCreateKeyExA	
HKEY_CURRENT_USER\Software\Microsoft\VB\7.0\Commo	success or wait	1	6E52A5E3	RegCreateKeyExA	
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	6E550648	unknown	
HKEY_CURRENT_USER\Software\Microsoft\Office\Commo\Offline\Options	success or wait	1	6E550648	unknown	
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	success or wait	1	6E550648	unknown	
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Commo\Recent Locations	success or wait	1	6E550648	unknown	
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Commo\Recent Locations\SharePoint	success or wait	1	6E550648	unknown	
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	6E550648	unknown	
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	6E550648	unknown	
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\34B33	success or wait	1	6E550648	unknown	
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	6E550648	unknown	
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	6E550648	unknown	
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\352A2	success or wait	1	6E550648	unknown	

Key Value Created							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	lx{	binary	21 78 28 00 64 07 00 00 02 00 00 00 00 00 00 00 5C 00 00 00 01 00 00 00 2C 00 00 00 24 00 00 00 73 00 61 00 6D 00 70 00 6C 00 65 00 32 00 30 00 32 00 32 00 30 00 31 00 32 00 34 00 2D 00 30 00 31 00 2E 00 78 00 6C 00 73 00 00 00 73 00 61 00 6D 00 70 00 6C 00 65 00 32 00 30 00 32 00 32 00 30 00 31 00 32 00 34 00 2D 00 30 00 31 00 00 00	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9275373402.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5713452101.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6422942404.xlsx	success or wait	1	6E550648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 4	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\3024948866.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 5	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\9655434068.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 6	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\1287572840.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 7	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\8182259827.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 8	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\6750529025.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 9	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\6109303877.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 10	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\9925478147.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 11	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\5491630718.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 12	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\9659692161.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 13	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\0653671941.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 14	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\1237160943.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 15	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\0450125302.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 16	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\6329227256.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 17	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\6183211589.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 18	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\7457734050.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 19	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\1141274626.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 20	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\9329238007.xlsx	success or wait	1	6E550648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5713452101.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6422942404.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3024948866.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9655434068.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1287572840.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8182259827.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6750529025.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6109303877.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9925478147.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5491630718.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9659692161.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0653671941.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1237160943.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0450125302.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6329227256.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6183211589.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7457734050.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1141274626.xlsx	success or wait	1	6E550648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\filemru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9329238007.xlsx	success or wait	1	6E550648	unknown

