ID: 504678
Sample Name:
004192374854_4.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 14:34:31
Date: 18/10/2021
Version: 33.0.0 White Diamond

Table of Contents

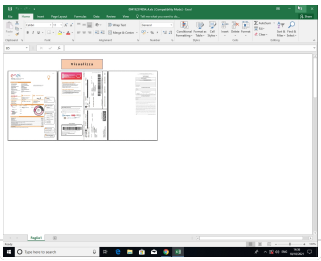
Windows Analysis Report 004192374854_4.xls

Overview

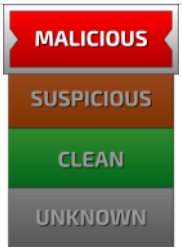
General Information

Sample Name:	004192374854_4.xls
Analysis ID:	504678
MD5:	f480fc1afe995ae…
SHA1:	441f53d97186305.
SHA256:	d29f6c42fa70b46..
Infos:	

Most interesting Screenshot:



Detection



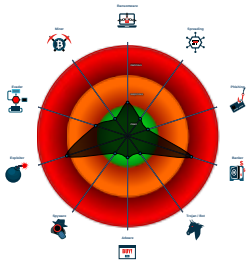
Ursnif Dropper

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

Signatures

- Multi AV Scanner detection for subm…
- Detected Italy targeted Ursnif droppe…
- Document contains an embedded VB…
- Document contains embedded VBA …

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6832 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

E-Banking Fraud:

Detected Italy targeted Ursnif dropper document

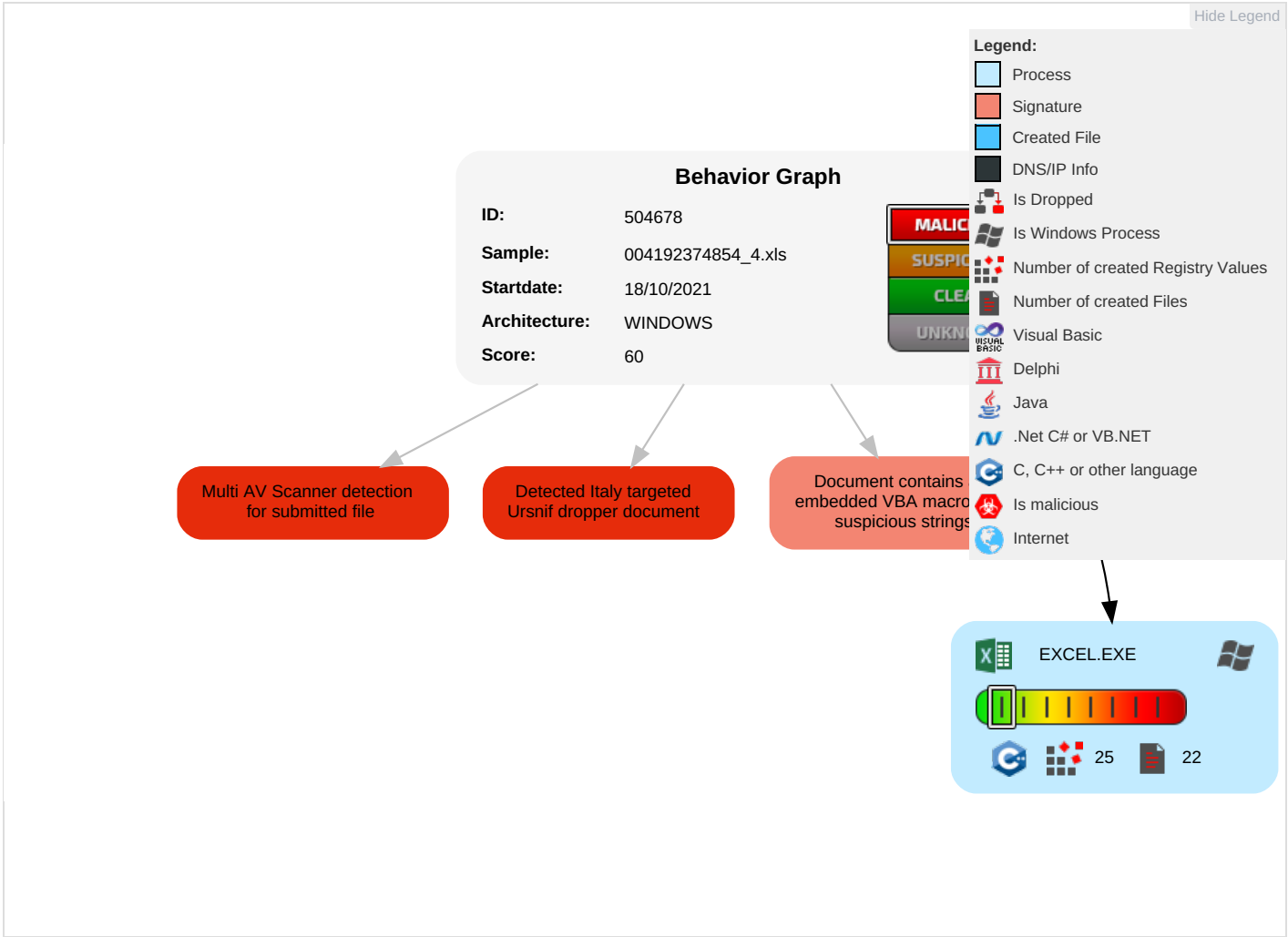
System Summary:

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	Scripting 1 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	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	Scripting 1 1	LSASS Memory	System Information Discovery 2	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

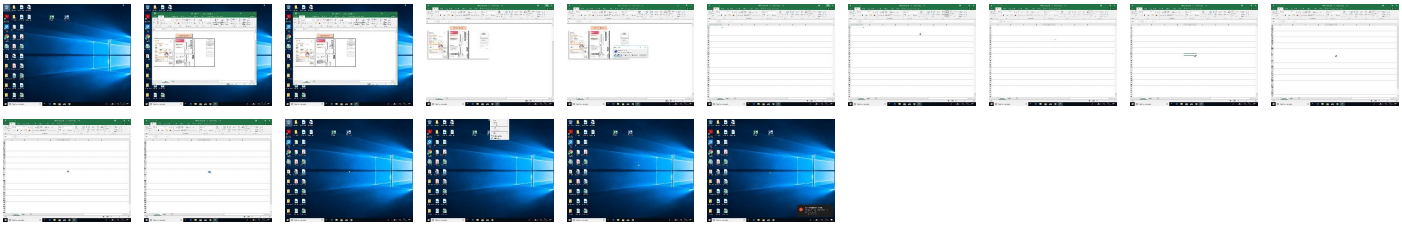
Behavior Graph

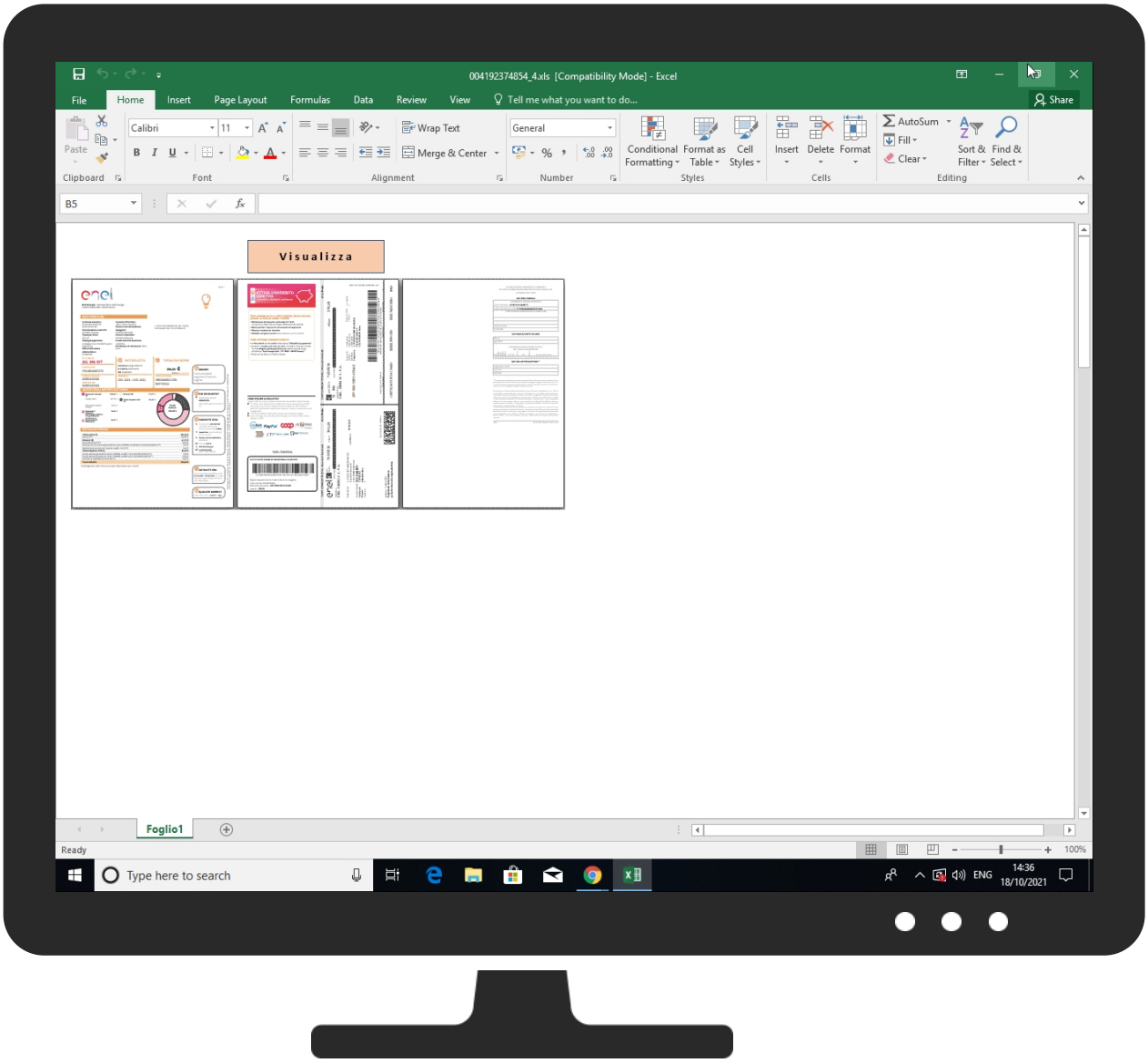


Screenshots

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
004192374854_4.xls	9%	Virustotal		Browse
004192374854_4.xls	3%	Metadefender		Browse
004192374854_4.xls	11%	ReversingLabs	Script.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
windowsupdate.s.llnwi.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
windowsupdate.s.llnwi.net	178.79.242.0	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	504678
Start date:	18.10.2021
Start time:	14:34:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	004192374854_4.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	19
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:	mal60.bank.expl.winXLS@1/1@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 • Changed system and user locale, location and keyboard layout to Italian - Italy • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active Picture Object • Active AutoShape Object • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
windowsupdate.s.llnwi.net	V5CfwElS7F.exe	Get hash	malicious	Browse	• 178.79.242.0
	a2YLQb35T6.exe	Get hash	malicious	Browse	• 178.79.242.128
	OmniCAD.dll	Get hash	malicious	Browse	• 178.79.242.128
	Lf7IXAF0Zd.exe	Get hash	malicious	Browse	• 178.79.242.0

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FACTURA 10172021B35646INV.exe	Get hash	malicious	Browse	• 178.79.242.0
	87R65JT93I.exe	Get hash	malicious	Browse	• 178.79.242.0
	004199280339_4.xls	Get hash	malicious	Browse	• 178.79.242.128
	SecuriteInfo.com.Trojan.Inject4.17696.9430.exe	Get hash	malicious	Browse	• 178.79.242.128
	DOCU6309491220 Telex release.exe	Get hash	malicious	Browse	• 178.79.242.128
	tvnserver.dll	Get hash	malicious	Browse	• 178.79.242.128
	jqfxgC51Ee.exe	Get hash	malicious	Browse	• 178.79.242.0
	bYHmn5GaOW.exe	Get hash	malicious	Browse	• 178.79.242.0
	MArqvsIOah.exe	Get hash	malicious	Browse	• 178.79.242.128
	lFs5dtof6Z.exe	Get hash	malicious	Browse	• 95.140.230.128
	QHD7nGySKa.exe	Get hash	malicious	Browse	• 178.79.242.128
	hoPVJ9kkds.exe	Get hash	malicious	Browse	• 178.79.242.128
	hoPVJ9kkds.exe	Get hash	malicious	Browse	• 178.79.242.128
	yDRpwgtz7p.exe	Get hash	malicious	Browse	• 178.79.242.128
	xEQtbX638l.exe	Get hash	malicious	Browse	• 178.79.242.128
	Vdslzshvovgybkzgrzotcepodrxkmdpxtj.exe	Get hash	malicious	Browse	• 178.79.242.128

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\A58416D3-19ED-4E1C-BD92-401540FA0C34	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	138049
Entropy (8bit):	5.359417618636917
Encrypted:	false
SSDEEP:	1536:rcQIKNZrBdA3gBwfnQ9DQW+zBY34Zzi7nXboOidXVE6LWME9:/WQ9DQW+zbXa1
MD5:	08A71D995E3E07D06F1F9DC41E9829A3
SHA1:	9D75C834E012C8EAACB2833CEB0CE9ADC400458C
SHA-256:	EBD9FC25B44972D9AFA30931E13F0E586AFF4D4EC7127D5744F80CADBE4B99A6
SHA-512:	5C46D3EDA38B1EB8D89E07926C8C310864127CB704DD90DDB2AC1A526D1FFD2B4021E138EDFA9923DDC0F4103D34384D7092FDFEB960B0CF0792BF18A5115EC
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-10-18T12:35:31">.. Build: 16.0.14612.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Create Time/Date: Mon Oct 18 10:07:46 2021, Last Saved Time/Date: Mon Oct 18 10:09:47 2021, Security: 0, Comments: Enel Energia - Mercato libero dell'energia

General

Entropy (8bit):	6.0128480654935625
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	004192374854_4.xls
File size:	59904
MD5:	f480fc1afe995ae4cafcb89b83295d88
SHA1:	441f53d97186305891267b6b98382f2a0fa180b7
SHA256:	d29f6c42fa70b462166272142d33012c41c471ea2c02943fae147fbccd5420aa
SHA512:	b5ea9a01308a6b84d89ba573a0a1957c448ea9e126323e748dfdae1caafbeed67d88188e3256799c40b5c0665370ff65985a41c38a0cdd2ff6fc6d30000c85f5
SSDEEP:	1536:SsQlYkElbSkKBEqEXPgsRZmbaoFhZhR0cixIHm0zCoyp6p2UUaVgO8f4QmMC:ShlYkEIuPm3fNRZmbaoFhZhR0cixIHm6
File Content Preview:	.....>.....M..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "004192374854_4.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
Comments:	Enel Energia - Mercato libero dell'energia
Create Time:	2021-10-18 09:07:46.324000
Last Saved Time:	2021-10-18 09:09:47
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

Streams

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 6832 Parent PID: 744

General

Start time:	14:35:29
Start date:	18/10/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x960000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis