

JoeSandbox Cloud BASIC



**ID:** 504678

**Sample Name:**

004192374854\_4.xls

**Cookbook:**

defaultwindowsofficecookbook.jbs

**Time:** 14:29:13

**Date:** 18/10/2021

**Version:** 33.0.0 White Diamond


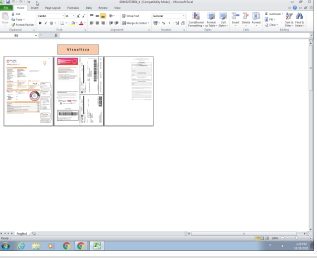
## Table of Contents

Table of Contents	2
Windows Analysis Report 004192374854_4.xls	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Jbx Signature Overview	3
AV Detection:	3
E-Banking Fraud:	4
System Summary:	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	5
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	6
Contacted Domains	6
Contacted IPs	6
General Information	6
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	7
IPs	7
Domains	7
ASN	7
JA3 Fingerprints	7
Dropped Files	7
Created / dropped Files	7
Static File Info	7
General	7
File Icon	8
Static OLE Info	8
General	8
OLE File "004192374854_4.xls"	8
Indicators	8
Summary	8
Document Summary	8
Streams with VBA	8
Streams	8
Network Behavior	8
Code Manipulations	9
Statistics	9
System Behavior	9
Analysis Process: EXCEL.EXE PID: 2576 Parent PID: 596	9
General	9
File Activities	9
File Created	9
File Deleted	9
File Moved	9
Registry Activities	9
Key Created	9
Key Value Created	9
Disassembly	9
Code Analysis	9

# 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

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

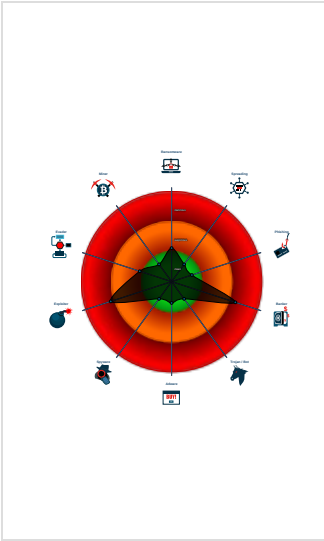
Ursnif Dropper

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 w7x64
-  EXCEL.EXE (PID: 2576 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

 Click to jump to signature section

AV Detection:



## E-Banking Fraud:



Detected Italy targeted Ursnif dropper document

## System Summary:

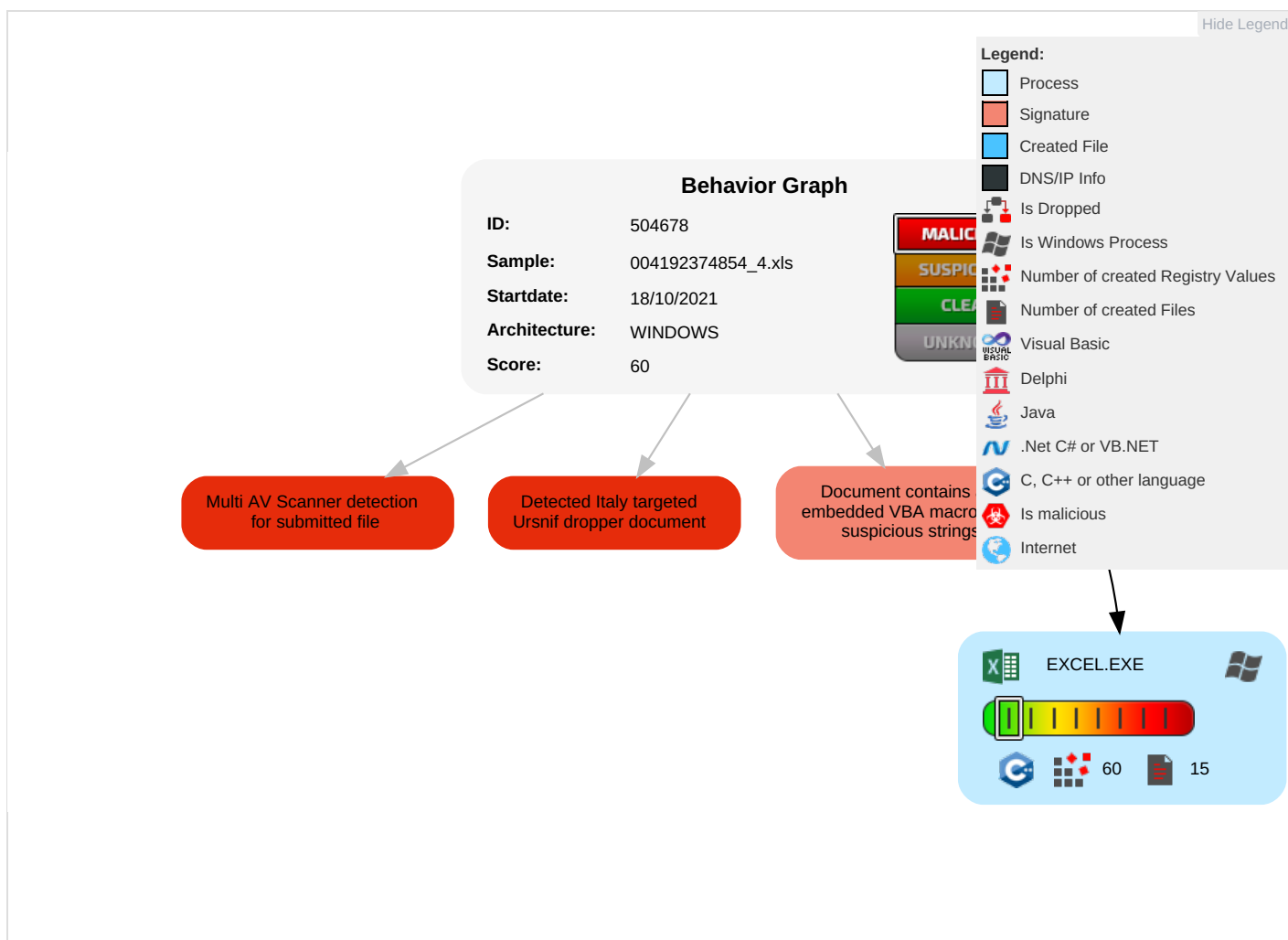


Document contains an embedded VBA macro with suspicious strings

## Mitre Att&amp;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	Scripting 1 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	Rootkit	LSASS Memory	System Information Discovery 1	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

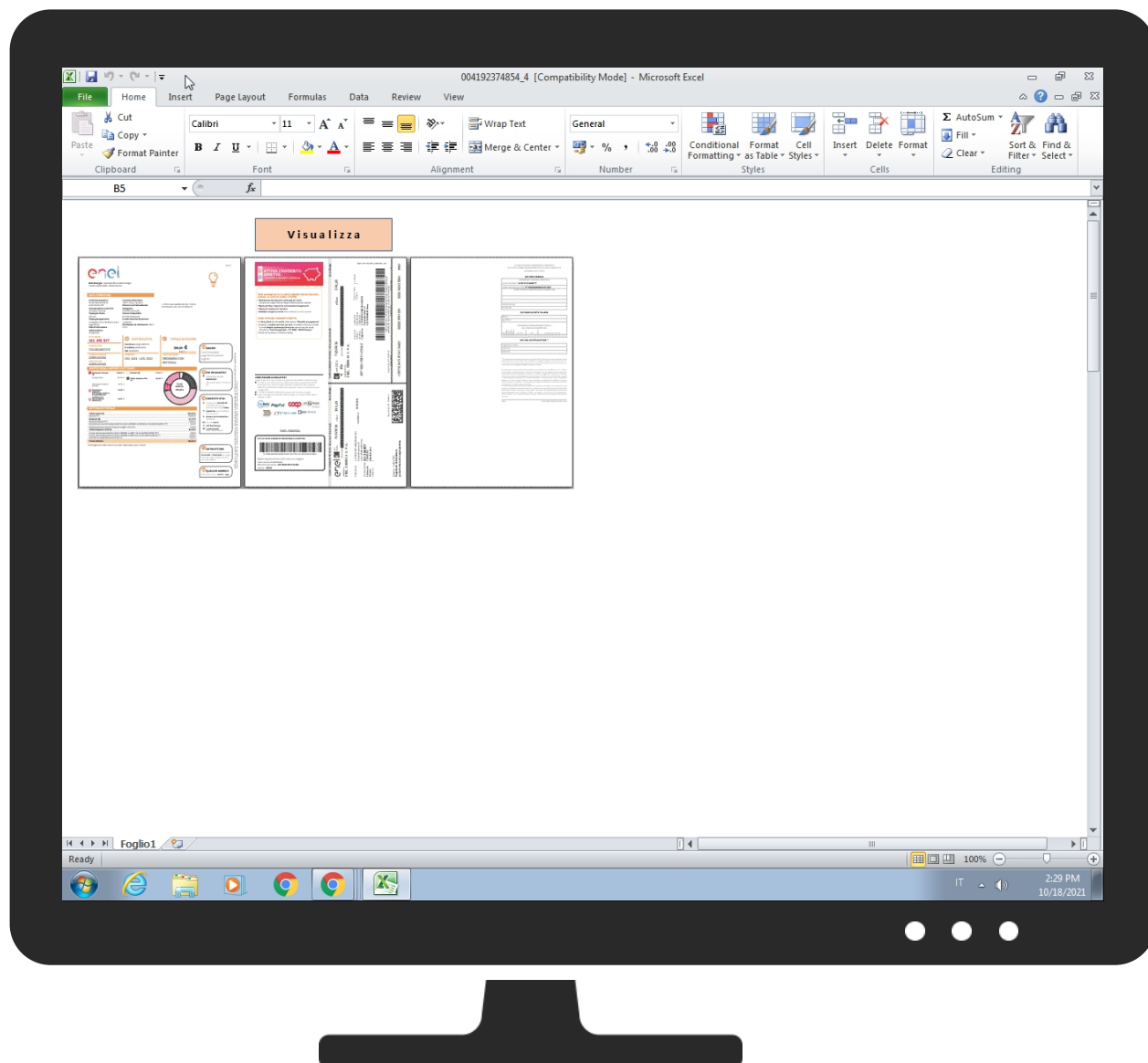
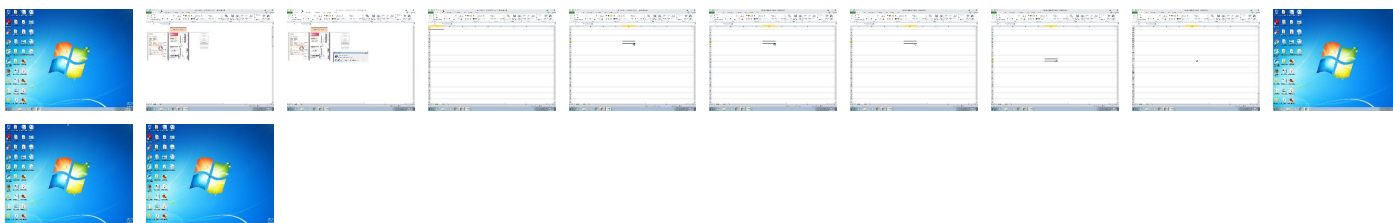
## Behavior Graph



## 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		<a href="#">Browse</a>
004192374854_4.xls	3%	Metadefender		<a href="#">Browse</a>
004192374854_4.xls	11%	ReversingLabs	Script.Trojan.Heuristic	

### 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

### 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:	14:29:13
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 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:	<ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.bank.expl.winXLS@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 100%</li><li>• Number of executed functions: 0</li><li>• Number of non-executed functions: 0</li></ul>

Cookbook Comments:	<ul style="list-style-type: none"> <li>• Adjust boot time</li> <li>• Enable AMSI</li> <li>• Found application associated with file extension: .xls</li> <li>• Changed system and user locale, location and keyboard layout to Italian - Italy</li> <li>• Found Word or Excel or PowerPoint or XPS Viewer</li> <li>• Attach to Office via COM</li> <li>• Active Picture Object</li> <li>• Active AutoShape Object</li> <li>• Scroll down</li> <li>• Close Viewer</li> </ul>
Warnings:	Show All

## Simulations

### Behavior and APIs

No simulations

## Joe Sandbox View / Context

### IPs

No context

### Domains

No context

### ASN

No context

### JA3 Fingerprints

No context

### Dropped Files

No context

## Created / dropped Files

No created / dropped files found


## Static File Info

General	
File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, 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
Entropy (8bit):	6.0128480654935625
TrID:	<ul style="list-style-type: none"> <li>• Microsoft Excel sheet (30009/1) 78.94%</li> <li>• Generic OLE2 / Multistream Compound File (8008/1) 21.06%</li> </ul>
File name:	004192374854_4.xls

## General

File size:	59904
MD5:	f480fc1afe995ae4cafc89b83295d88
SHA1:	441f53d97186305891267b6b98382f2a0fa180b7
SHA256:	d29f6c42fa70b462166272142d33012c41c471ea2c02943fae147fbccd5420aa
SHA512:	b5ea9a01308a6b84d89ba573a0a1957c448ea9e126323e748dfdae1caafbeed67d88188e3256799c40b5c0665370ff65985a41c38a0cdd2ff6fc6d30000c85f5
SSDEEP:	1536:SsQIYkElbSkKBEqEXPgSRZmbaoFhZhR0cixlHm0zCoyp6p2UUaVgO8f4QmMC:ShlYkEluPm3fNRZmbaoFhZhR0cixlHm6
File Content Preview:	.....>.....M..... ..... .....

## File Icon

	
Icon Hash:	e4eea286a4b4bcb4

## 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: 2576 Parent PID: 596

General

Start time:	14:29:21
Start date:	18/10/2021
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:	0x13f2d0000
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

Show Windows behavior

File Created

File Deleted

File Moved

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis