JoeSandbox Cloud BASIC

ID: 509333
Sample Name:
aaaaaaaaaaa.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:19:09
Date: 26/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

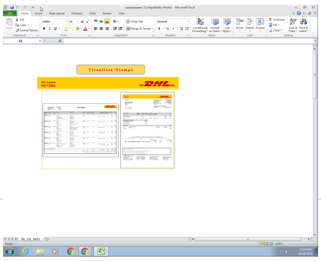
Windows Analysis Report aaaaaaaaaaa.xls

Overview

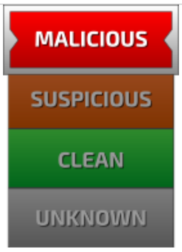
General Information

Sample Name:	aaaaaaaaaaa.xls
Analysis ID:	509333
MD5:	a8ca4b1a0ab594..
SHA1:	2e8c2f19a0a5875.
SHA256:	9cb3b49716b637..
Tags:	xls
Infos:	

Most interesting Screenshot:



Detection



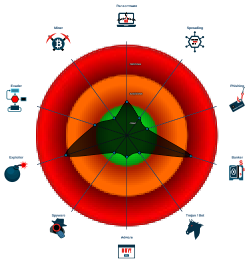
Ursnif Dropper

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 w7x64**
- EXCEL.EXE (PID: 2016 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:

Multi AV Scanner detection for submitted file

Copyright Joe Security LLC 2021

E-Banking Fraud:

Detected Italy targeted Ursnif dropper document

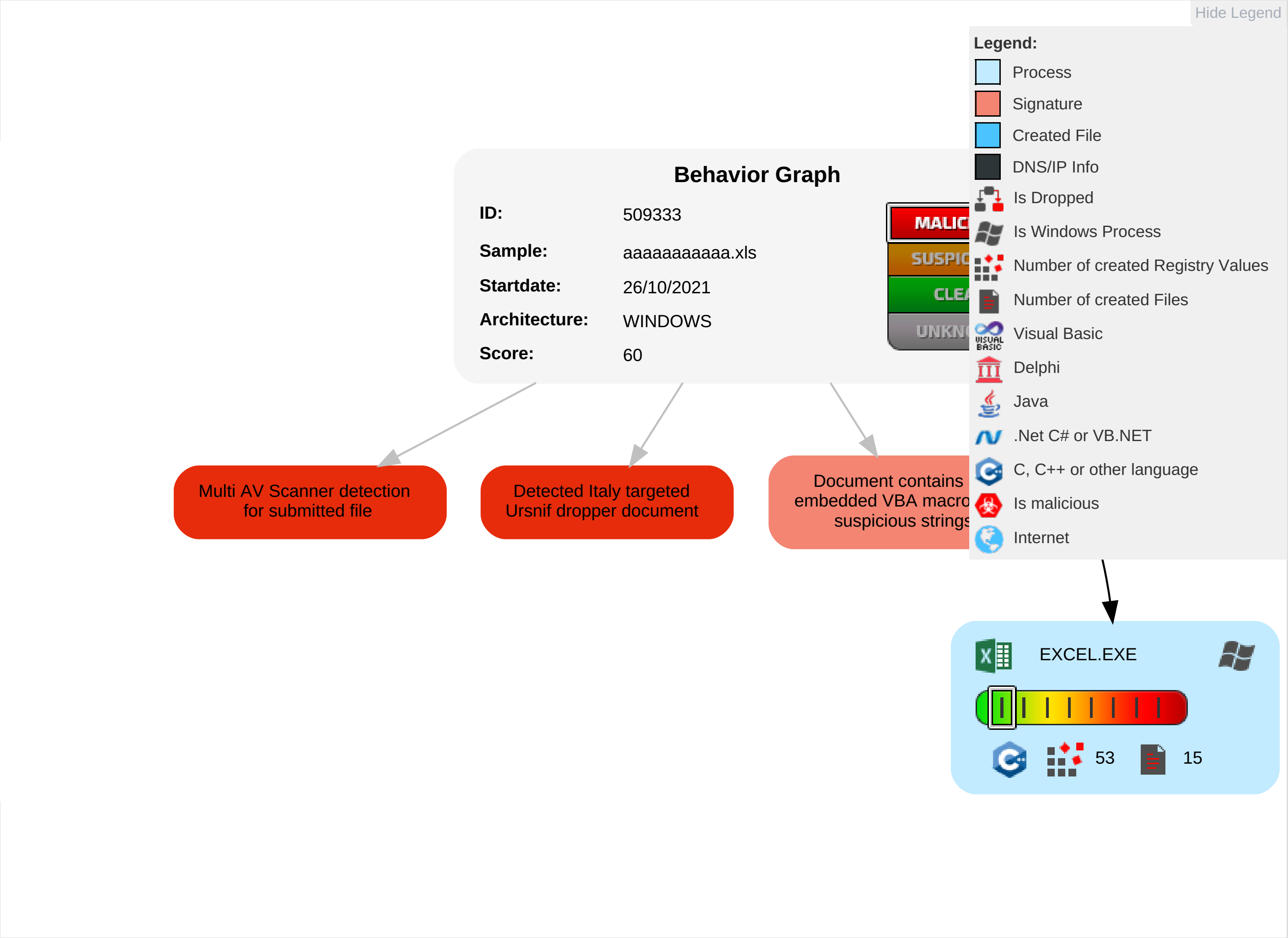
System Summary:

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	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



Behavior Graph

ID: 509333

Sample: aaaaaaaaaaa.xls

Startdate: 26/10/2021

Architecture: WINDOWS

Score: 60

Legend:

□	Process
🟥	Signature
🟦	Created File
■	DNS/IP Info
	Is Dropped
	Is Windows Process
	Number of created Registry Values
	Number of created Files
	Visual Basic
	Delphi
	Java
	.Net C# or VB.NET
	C, C++ or other language
	Is malicious
	Internet

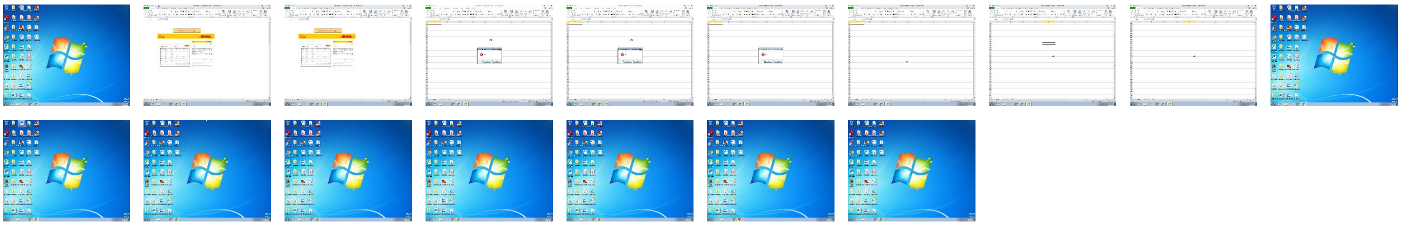
Hide Legend
MALIC
SUSPIC
CLEA
UNKN
Multi AV Scanner detection for submitted file
Detected Italy targeted Ursnif dropper document
Document contains embedded VBA macro suspicious strings
EXCEL.EXE
53
15

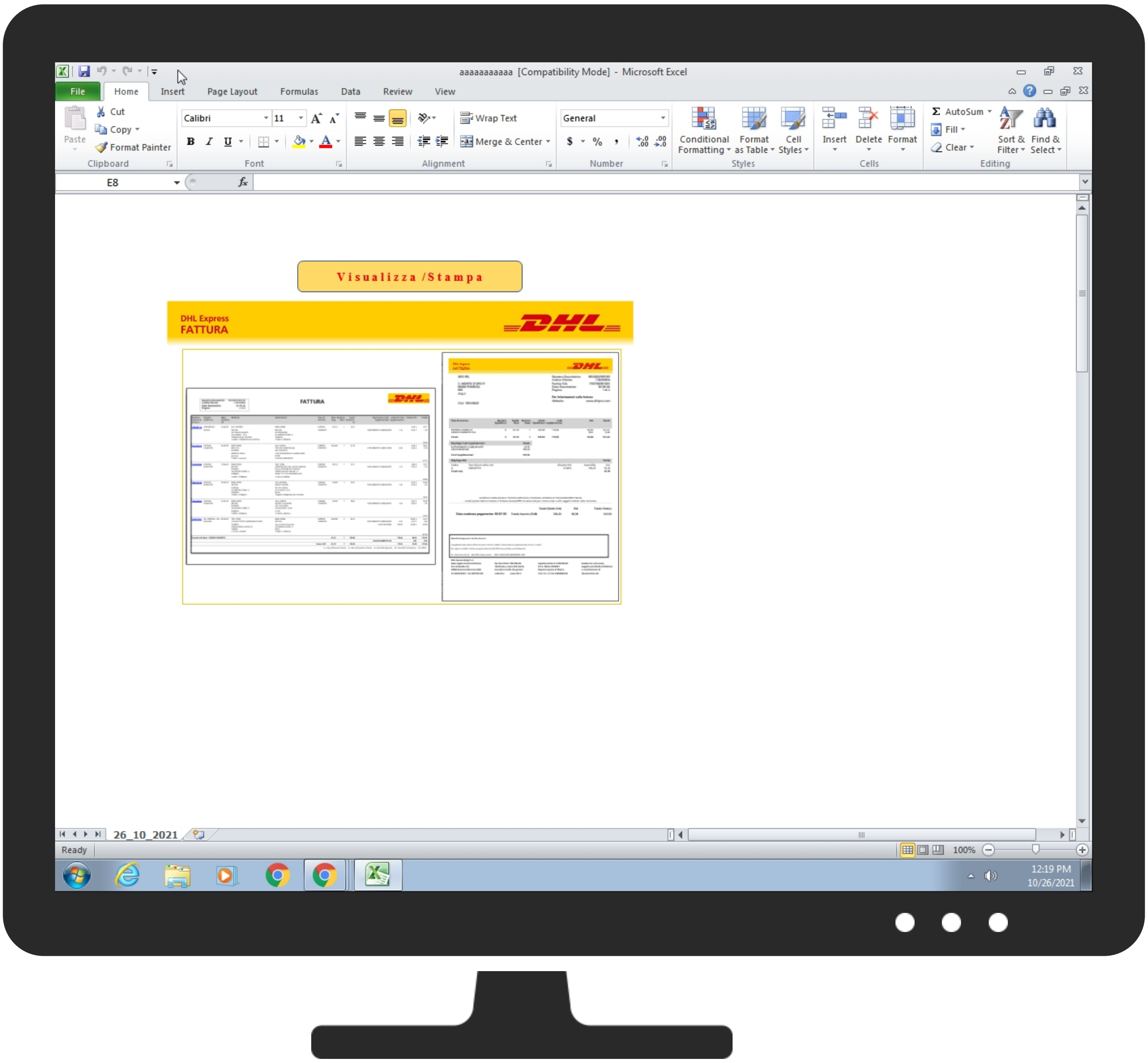
Copyright Joe Security LLC 2021

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
aaaaaaaaaaa.xls	14%	Virustotal		Browse

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:	509333
Start date:	26.10.2021
Start time:	12:19:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	aaaaaaaaaaa.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:	mal60.bank.expl.winXLS@1/0@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 AutoShape Object • Scroll down • Close Viewer
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: Tue Oct 26 08:18:26 2021, Last Saved Time/Date: Tue Oct 26 08:18:28 2021, Security: 0
Entropy (8bit):	5.783981035047647
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	aaaaaaaaaaa.xls
File size:	56320
MD5:	a8ca4b1a0ab594b286145586e6b4921c
SHA1:	2e8c2f19a0a58755d03bcf12a38e9383d49a8465
SHA256:	9cb3b49716b637ee57db8cc7bd17189ac2fa2489d8ba32a94a7c99f20fa82a5e
SHA512:	42cf117b13e4e972f5565016f92bed73d915dccccb8f7e929ce6850c47dd4befe4dcd8723d6b124fd8f82c5f7da631b54fa4f820b56223b8e41397a73650c6cd
SSDEEP:	1536:FsQlYkEIbSkKBEqEXPgsRZmbaoFhZhR0cixIHm0205bQK/6wP6mMCWtmKl:FhlYkEIuPm3fNRZmbaoFhZhR0cixIHmp

General	
File Content Preview:	........................>..................................F..

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "aaaaaaaaaaa.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:	
Last Saved By:	
Create Time:	2021-10-26 07:18:26.189000
Last Saved Time:	2021-10-26 07:18:28
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

Copyright Joe Security LLC 2021

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 2016 Parent PID: 596

General

Start time:	12:19:16
Start date:	26/10/2021
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:	0x13f140000
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

Copyright Joe Security LLC

Joe Sandbox Cloud Basic 33.0.0 White Diamond