ID: 491709
Sample Name:
Faturados_Externo_26_09.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:26:44
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

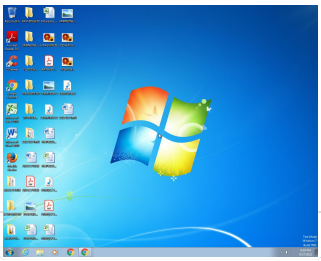
Windows Analysis Report Faturados_Externo_26_09.xls

Overview

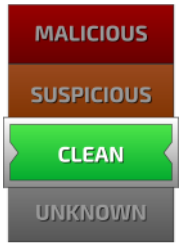
General Information

Sample Name:	Faturados_Externo_26_09.xls
Analysis ID:	491709
MD5:	bb5c37e33e7e1fb.
SHA1:	03066751e384c6..
SHA256:	002b87472b1991..
Tags:	geo PRT xls
Infos:	

Most interesting Screenshot:



Detection

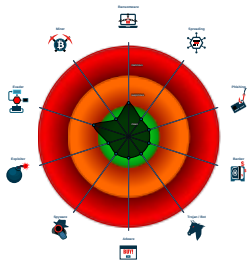


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Document contains an embedded VB...

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 512 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

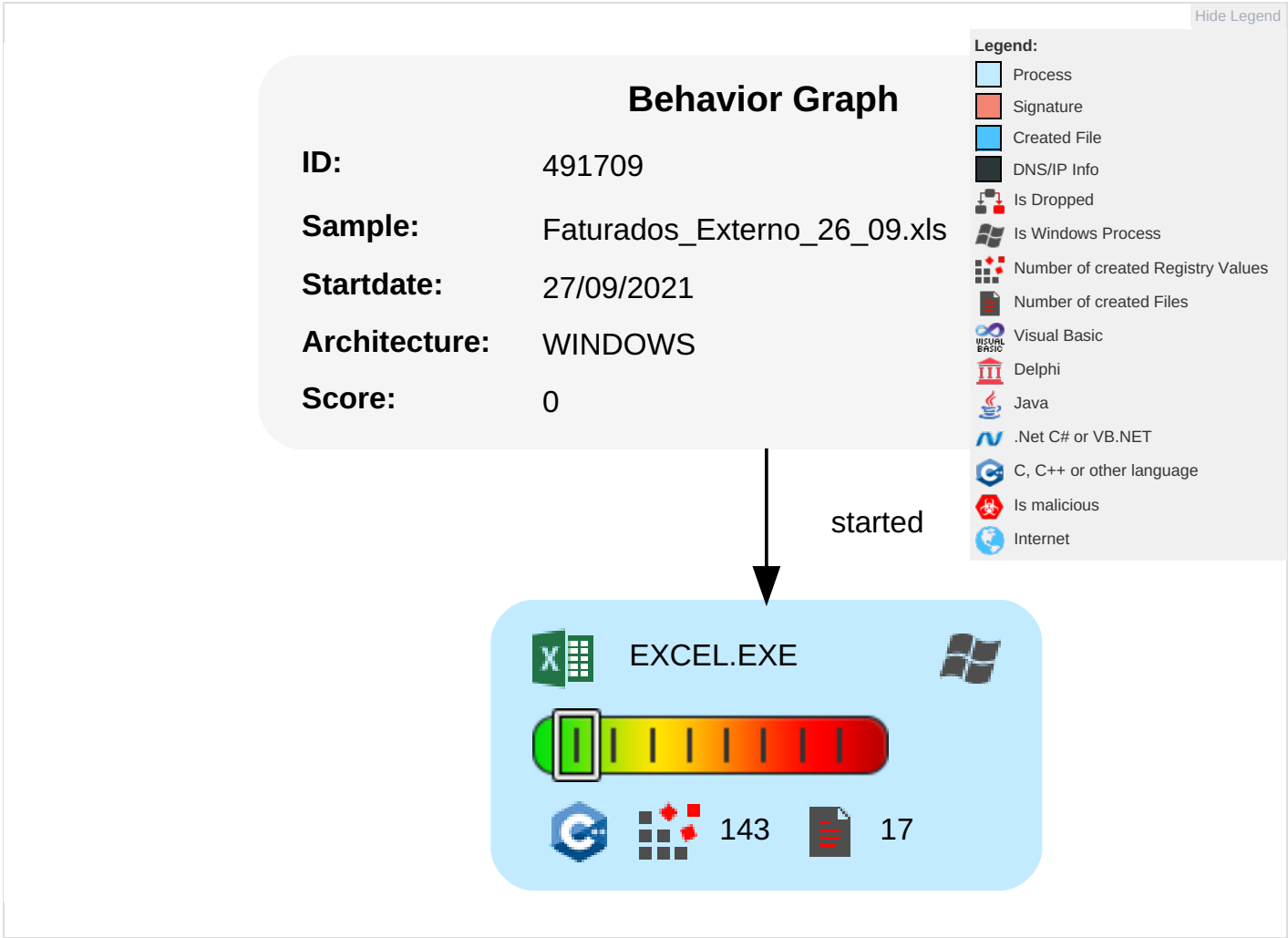
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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	Path Interception	Path Interception	Scripting 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	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

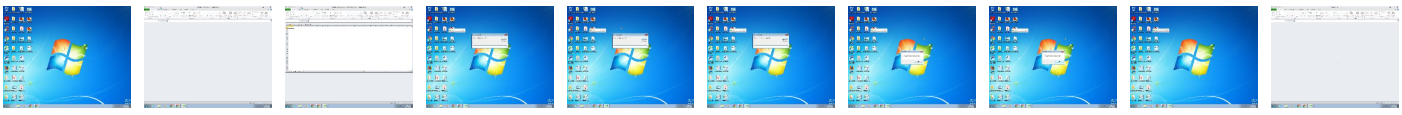
Behavior Graph



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
Faturados_Externo_26_09.xls	0%	Virustotal		Browse
Faturados_Externo_26_09.xls	0%	ReversingLabs		

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:	491709
Start date:	27.09.2021
Start time:	20:26:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Faturados_Externo_26_09.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:	• EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winXLS@1/3@0/0
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 • 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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\251D90EB.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	2804
Entropy (8bit):	2.6224368355147445
Encrypted:	false
SSDEEP:	24:YAtE+Y0xEjrlbDK3XHqYdV7C2tEDEcq4nJssdCqzvYDy22PEnOds6gAMToFM166q:dmDKnZJdtJcqCJssdCqzvy7imTo
MD5:	14FC01BED46EB78EB1F149A96B852DBF
SHA1:	156279B5667F0ECFC5ECC1E73E6F5F6B0AB2FCBD
SHA-256:	BC79B5AF0298E761109C737731B9832513C86254DC84CABFD6C2C93C813E3A42
SHA-512:	97E0CE4DA26D7239A43F8590E4BBF86FD4C90DE60D8D4F8F9AD9176E4F0F21A5147D4A3B01CC06D9080F4682975C7179D67C9DE6EA1B8CB779918AAFBE4F8DE
Malicious:	false
Reputation:	low
Preview:	....l.....(..... EMF.....2.....V.....5.....F...`...R...GDIC.....5<....:.....).....).....iii.....-.....!...).....!.....(.....-.....!...(.....!.....-.....!...'.....!.....'.....-.....!...&.....!.....-.....!...%.....-.....!...#.....).....@..Arial.fR....._.....-.....)...2.....Atualizar base Input.....'.....).....).....).....)...!.....'.....iii.....%.....L...d.....(.....).....!.....?.....?.....L...d.....(.....(.....(.....!.....?.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B250F412.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	2708
Entropy (8bit):	2.5786874272687887
Encrypted:	false
SSDEEP:	24:YWtEK0iSjIEbAFl1dLMHoaYxD6xZ0Hv539Dv28fEhzds6gh/DA:LLEcFlDoIam53Be8wIE
MD5:	C44F1D185564C8F67F6AA4B5816D39C5
SHA1:	0C2824967371BED57208D775A41F27FA5F67076E
SHA-256:	0D97E2158715C2464899F235E76F91BAFBBF4ABEC8E4EA8B5854EC4D7AFE0E21
SHA-512:	1C7D6A91B45468FE64484D06AA5653D3CBB401B9E4C8F7D9B2083912526FF01BB96E7FFBABD0F62EA135EE603364684AEC1548A691850332A6FADBC1E5C67CE9
Malicious:	false
Reputation:	low
Preview:	....l.....~..... EMF.....2.....V.....5.....F...@...2...GDIC.....`.....iii.....-.....!.....!.....-.....!.....!.....-.....!.....!.....-.....!.....-.....!.....@..Arial.f.....;.....-.....2...(.....FINALIZAR.....'.....!.....'.....iii.....%.....L...d.....!.....?.....?.....L...d.....!.....?.....?.....

C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	241332
Entropy (8bit):	4.206827516046406
Encrypted:	false
SSDEEP:	1536:cGkfEQNSk8SCtKBX0Gpb2vxKHnVMOkOX0mRO/NIAIQK7viKAJYsA0ppDCLTfMRsi:ctBNSk8DtKBrpb2vxrOpprf/nVq
MD5:	336BB41F6CD1C326CD636B3816065996
SHA1:	0A0E998DA87EBA04C4DE79921067AD70323FCE62
SHA-256:	6F8259010B97BD1E613F9F5DECEB2EDD79D13EA476C8696831D0D1DE410F1B01
SHA-512:	CAD2C1690D984627A978CA759FB5B180EC71305AE3155A6B6F1FBE34089F6A2295E2DB6259E2482551602D453580A199778634D9BD4ACB7A4A0179E76EF9D25D
Malicious:	false
Reputation:	low
Preview:	MSFT.....Q.....$.....$..... .....d.....X..... .....L.....x.....@.....I.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....\|.....D.....p.....8.....d.....X..... .....L.....x.....@..... ..I ... ..4!...!..!..`"...".(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,..,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8..... H...4.....x...I.....T..... ..P..... ....&!..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: multibras eletrodomesticos, Last Saved By: HENRIQUE Tempesta, Name of Creating Application: Microsoft Excel, Create Time/Date: Wed Aug 27 14:16:27 2008, Last Saved Time/Date: Mon Sep 27 17:53:48 2021, Security: 1
Entropy (8bit):	7.504037198033761
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	Faturados_Externo_26_09.xls
File size:	6468096
MD5:	bb5c37e33e7e1fb9bb7b13960aad6b27
SHA1:	03066751e384c6b9c7df910cd01844f86cbaa43b
SHA256:	002b87472b1991ce420fbaccf76e14620aaf567ee11e2081a559dcefab05fef5
SHA512:	6c8b98b91e9ed390cd6b77ea3d0a077aefa6caf2465d6386574a0a7aa31a38163351b67c2eeb3962753c12eef510fb86a8880e30d63efaf158694e74286c5c59
SSDEEP:	196608:uQfhzNeEyOb5U4TzBLqKU7zgqTvFV21Xq1kYTqE3ZpMf1m+K+76P5veG2cn:npReEzdUVKUQqTvFV/1kYuEZKfs+p7AH
File Content Preview:	.....>.....c.....c.....e.....g.....i.....k.....m.....o.....q.....s.....u.....w.....y.....{.....}.....a.....c.....e.....g.....i.....k.....m.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 512 Parent PID: 596

General

Start time:	20:27:57
Start date:	27/09/2021
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:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly