ID: 491709
Sample Name:
Faturados_Externo_26_09.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:33:44
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

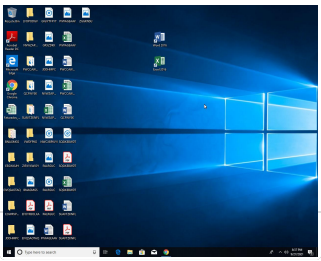
Windows Analysis Report Faturados_Externo_26_09.xls

Overview

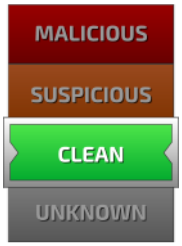
General Information

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

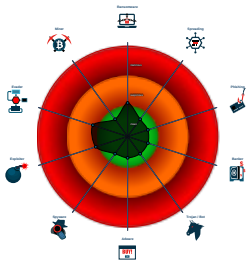


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Document contains an embedded VB...

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6344 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

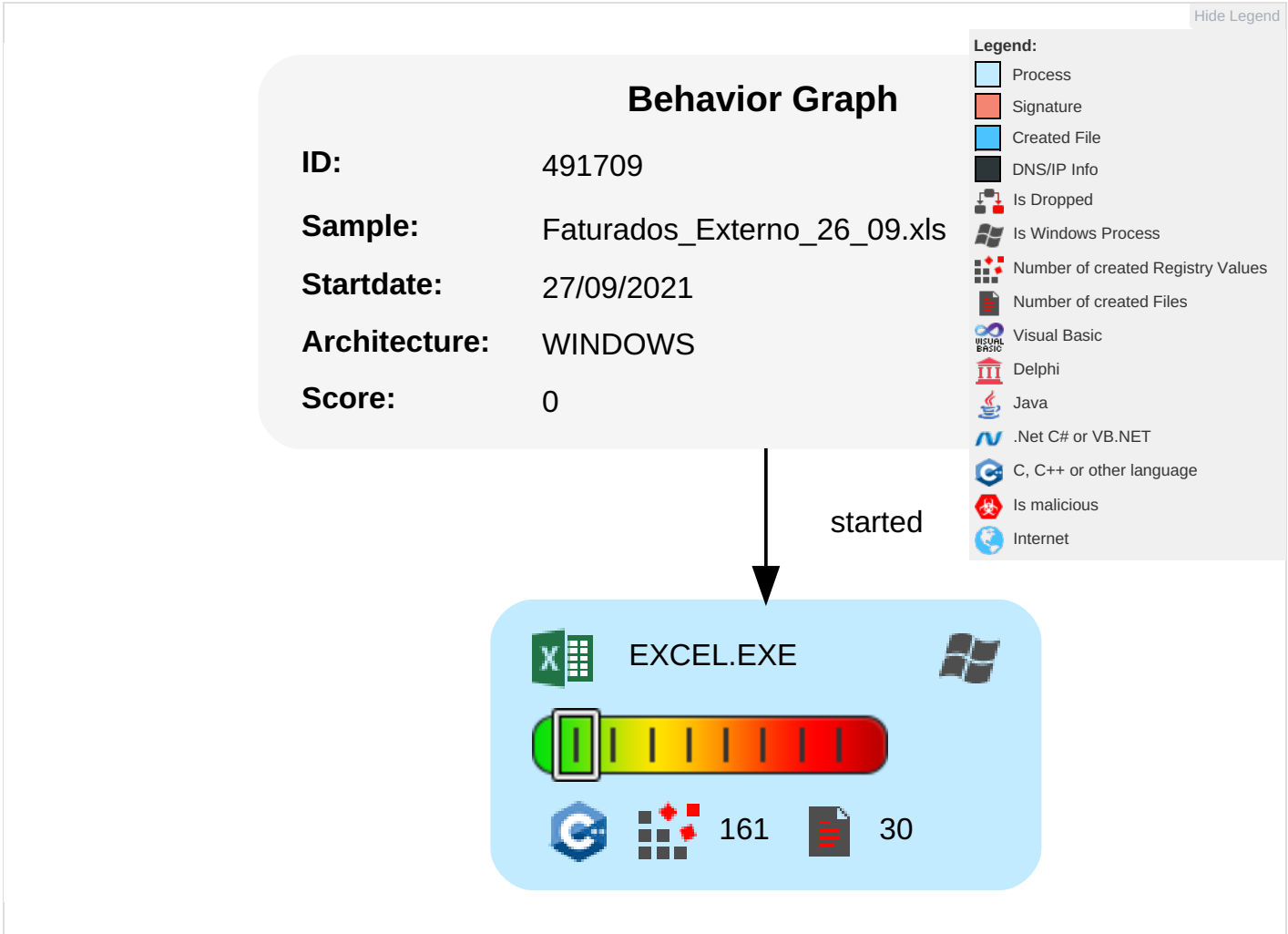
Click to jump to signature section

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	Impa
Valid Accounts	Scripting 1	Path Interception	Extra Window Memory Injection 1	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	Modif Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 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	Devic Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Extra Window Memory Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

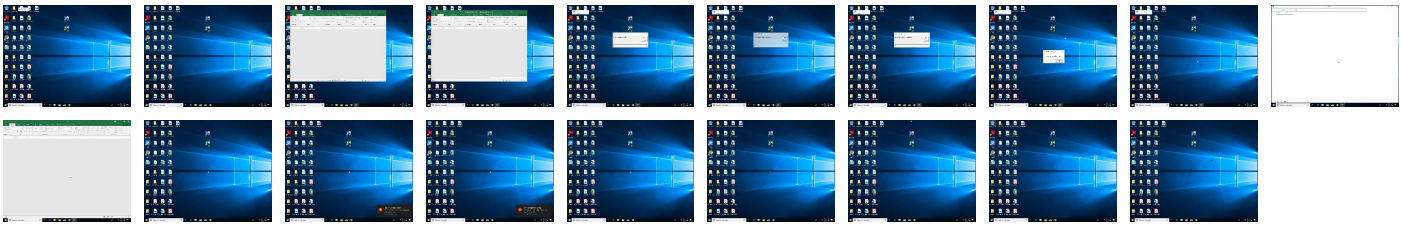
Behavior Graph



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%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

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://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-user.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://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	
http://https://augloop.office.com;https://augloop-gcc.office.com;https://augloop.gov.online.office365.us;ht	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

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:	20:33:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 41s
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 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:	11
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winXLS@1/4@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\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\1E49091D-2F41-4D12-AA8A-5E0F0E8C3392

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\1E49091D-2F41-4D12-AA8A-5E0F0E8C3392	
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	138701
Entropy (8bit):	5.360733266434256
Encrypted:	false
SSDEEP:	1536:+cQIKNZeBdA3gBwfnQ9DQW+z2Y34Zli7nXboOidX8E6LWME9:lWQ9DQW+z6Xh1
MD5:	EA5D73D20641058609F3ADE1067F1245
SHA1:	CC453919CCBBA61E77B8F621232E0299B0768010
SHA-256:	8A84ADAF927D4B7F7138C503757E957D5814C4E8B35093DA1FC5399D894DA1B1
SHA-512:	2E34A49C7482E2D125C3CCF65650B597D6DD894727667B78E37976E5E7FB194CC27518B10C9B352BD56B4422EE77CF1694A75B44654BD61C85E4CFCBE1EEB3A7
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="2021-09-27T18:35:23">.. Build: 16.0.14522.30525-->.. <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:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\77110AAA.emf	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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\INetCache\Content.MSO\7DA74C0D.emf	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:LLEcFlDoIam53Be8wlE
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 (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	248808
Entropy (8bit):	4.291083963049068

C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	
Encrypted:	false
SSDEEP:	3072:XzuSNQT8WZFVKKHSRDqBcA+FLM0Ar6t3s6bh:XzlNQAMFVTHSIcA+FLM0Awjbh
MD5:	55DF7CB1D2449438B44C234E2F035524
SHA1:	A5435D19D53BC5406A14D4D5473054CA24C07402
SHA-256:	4F02C73E5BE9C15EEE7E5A58DA8A662372F6EF276AC4E7E3D9C16ABB1F7078CE
SHA-512:	B9135D660C6399811DC02F4C77CDB143FB43E7C7ED1F573BEC6EB2562632E4B01626D5298F5E281D06BE8B88564DFE94233A32CC23F3E81AAA89137A9AC0DF3D
Malicious:	false
Reputation:	low
Preview:	MSFT.....Q.....%.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t..... <.....h.....0.....\.....$.....P.....|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..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...9..l9...9.. 4:...:...:..`;...;..(<...<...<..T=...=...>...>...>..H?...?...@..t@...@..<A...A...B..hB.....l...B.....H...4..... .....x..lL.....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:	74ecd4c6c3c6c4d8

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 6344 Parent PID: 792

General

Start time:	20:35:21
Start date:	27/09/2021
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:	0x1350000
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

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly