ID: 532474
Sample Name:
SCAN_7295943480515097.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:22:08
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

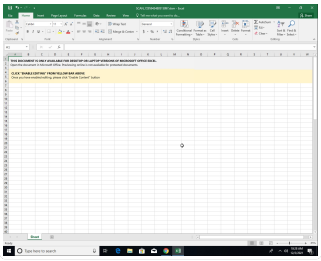
Windows Analysis Report SCAN_7295943480515097.xlsm

Overview

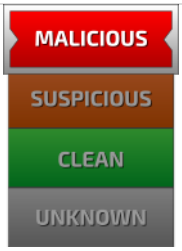
General Information

Sample Name:	SCAN_7295943480515097.xlsm
Analysis ID:	532474
MD5:	1ab11dce30326f3.
SHA1:	397dd88ca9d78a..
SHA256:	8f8e07b2eaca8af..
Infos:	

Most interesting Screenshot:



Detection



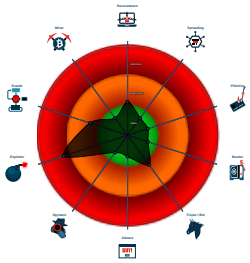
Hidden Macro 4.0

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Multi AV Scanner detection for subm…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Document exploit detected (UrlDown…
- Found a hidden Excel 4.0 Macro she…
- Potential document exploit detected…
- Uses a known web browser user age…
- Yara detected Xls With Macro 4.0
- JA3 SSL client fingerprint seen in co…
- Excel documents contains an embe…
- Potential document exploit detected…
- Potential document exploit detected…
- Document misses a certain OLE str…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 5980 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 3928 cmdline: C:\Windows\SysWow64\rundll32.exe ..\besta.ocx,44532.4348061343 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

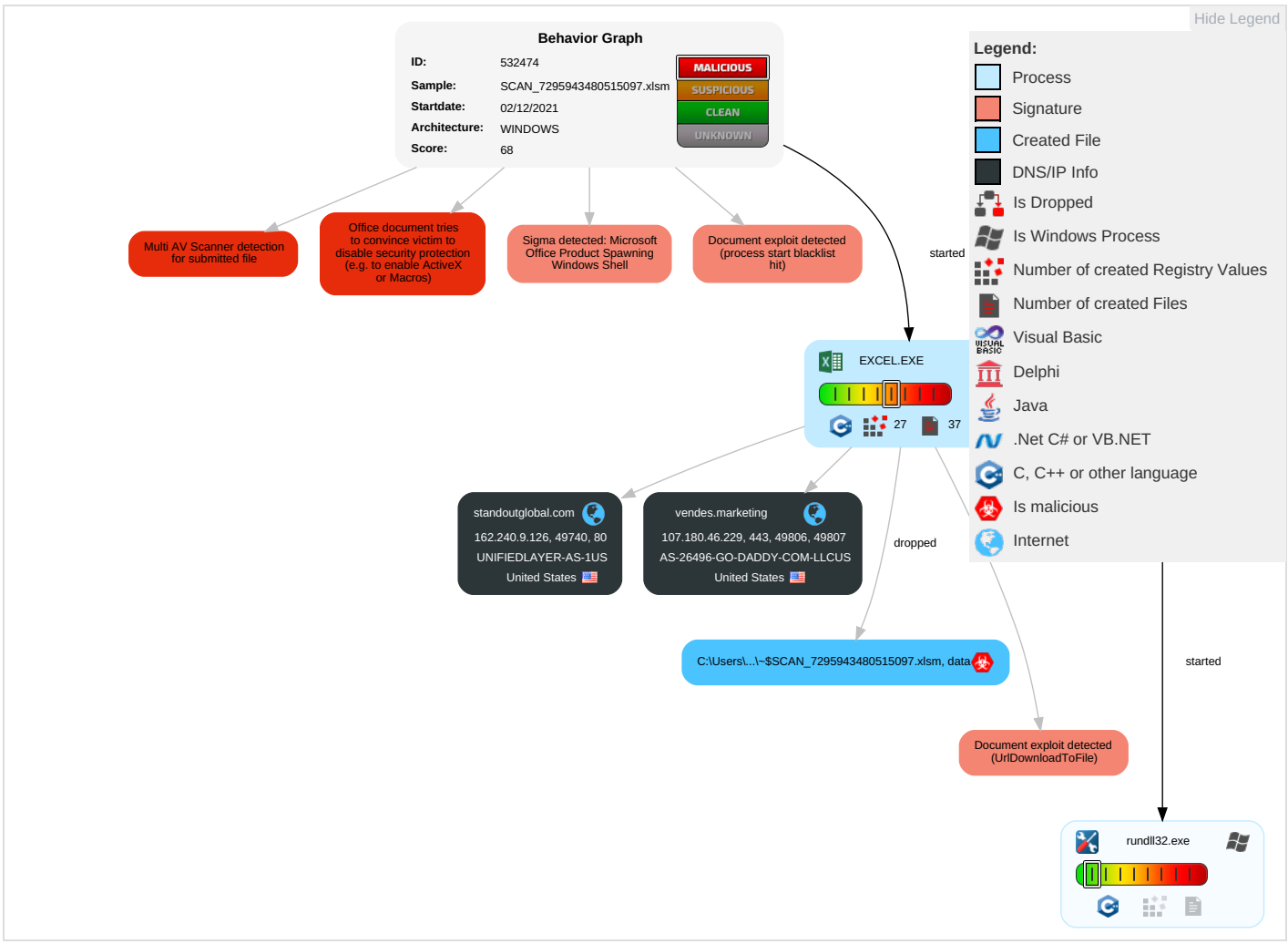
System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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	Im
Valid Accounts	Scripting 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap		Ca Bi Fr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M Ap Ra or

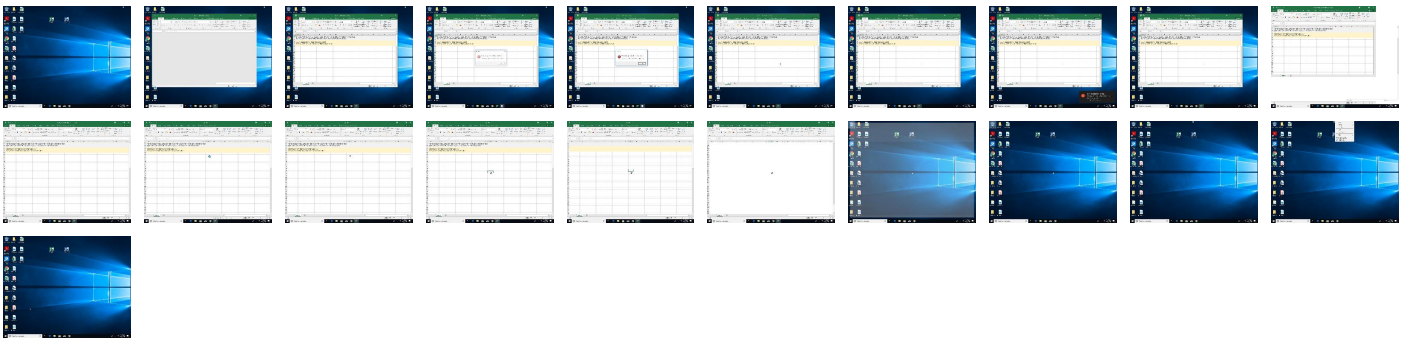
Behavior Graph

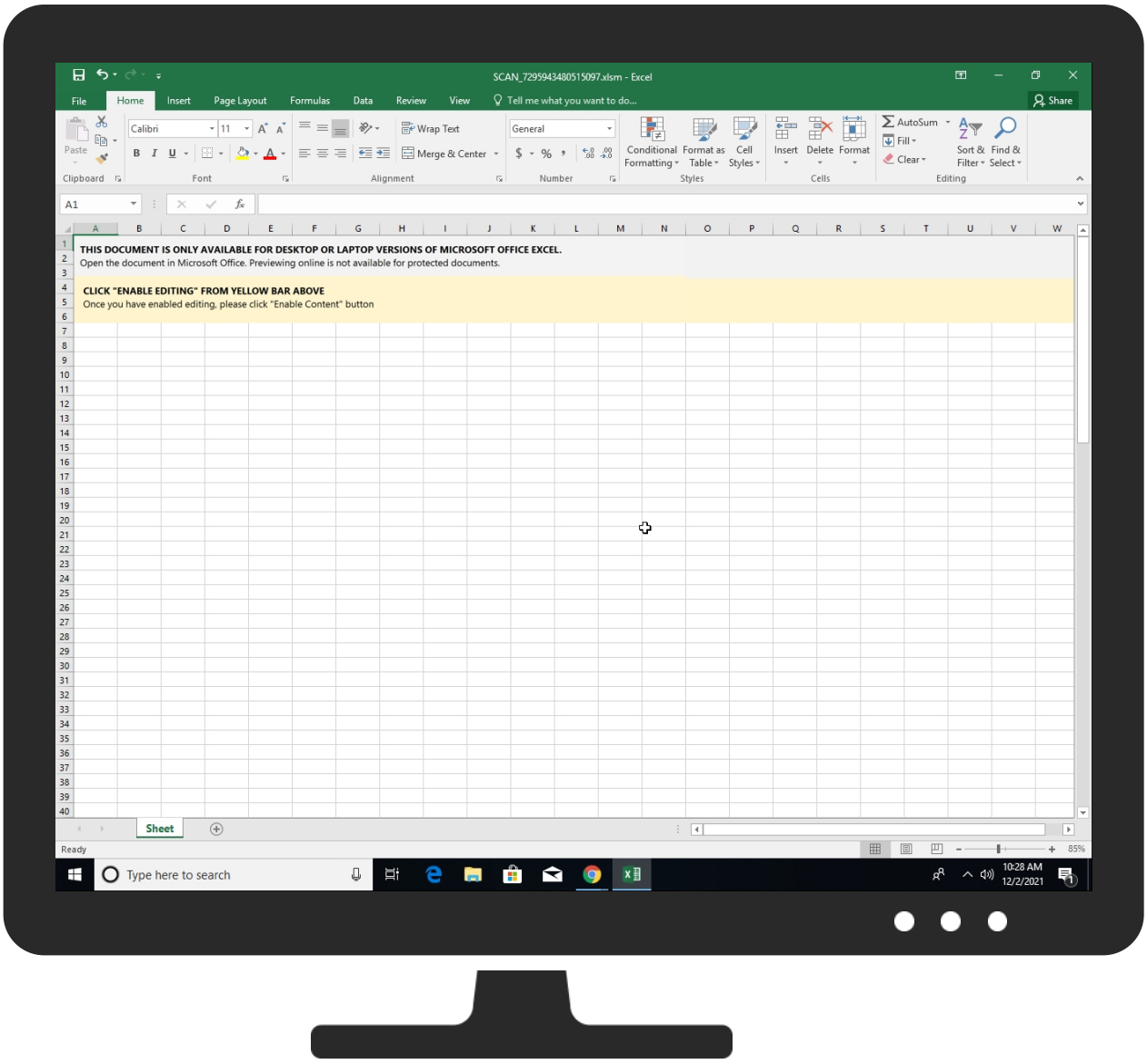


Screenshots

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
SCAN_7295943480515097.xlsm	22%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
standoutglobal.com	3%	Virustotal		Browse
vendes.marketing	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://vendes.marketing/wp-content/uploads/2021/10/framer.svg	0%	Avira URL Cloud	safe	
http://https://settings.outlook.comH	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://vendes.marketing/agencia-de-marketing-digital/e-commerce-efectivo/conversion-rate-optimizati	0%	Avira URL Cloud	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://vendes.marketing/wp-content/uploads/2021/11/logo-VNDSmkt-final-300x102.png	0%	Avira URL Cloud	safe	
http://https://vendes.marketing/wp-content/uploads/2021/10/anuncios-300x270.png	0%	Avira URL Cloud	safe	
http://https://vendes.marketing/wp-content/plugins/elementor/assets/lib/font-awesome/css/solid.min.css?ver=	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFileed	0%	Avira URL Cloud	safe	
http://https://vendes.marketing/wp-content/uploads/2021/10/visual-Studio.svg	0%	Avira URL Cloud	safe	
http://https://vendes.marketing/agencia-de-marketing-digital/servicios-de-marketing-digital/publicidad-digi	0%	Avira URL Cloud	safe	
http://vendes.marketing/transmigrant/Wplzr/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://vendes.marketing/agencia-de-marketing-digital/e-commerce-efectivo/tienda-online-con-magento/	0%	Avira URL Cloud	safe	
http://https://o365auditrealtimeingestion.manage.office.comP	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://vendes.marketing/wp-content/uploads/2021/10/figma.svg	0%	Avira URL Cloud	safe	
http://https://vendes.marketing/wp-content/plugins/elementor-pro/assets/css/frontend.min.css?ver=3.0.2	0%	Avira URL Cloud	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://vendes.marketing/agencia-de-marketing-digital/consultorias/consultoria-en-marketing-basado-e	0%	Avira URL Cloud	safe	
http://https://vendes.marketing/wp-content/uploads/elementor/css/post-2157.css?ver=1638212282	0%	Avira URL Cloud	safe	
http://https://vendes.marketing/wp-includes/css/dist/block-library/style.min.css?ver=5.8.2	0%	Avira URL Cloud	safe	
http://https://vendes.marketing/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fvendes.marketing%2F	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://augloop.office.comLinkRequestApiPageTitleRetrievalhttps://uci.	0%	Avira URL Cloud	safe	
http://https://vendes.marketing/wp-content/uploads/2021/10/elementor.svg	0%	Avira URL Cloud	safe	
http://https://vendes.marketing/wp-content/themes/twentytwentyone/assets/css/ie.css?ver=1.4	0%	Avira URL Cloud	safe	
http://https://vendes.marketing/wp-content/uploads/images/caso-exito1.png	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://vendes.marketing/agencia-de-marketing-digital/servicios-creativos/produccion-audiovisual/	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/?	0%	Avira URL Cloud	safe	
http://https://vendes.marketing/wp-content/uploads/2021/10/anuncios.png	0%	Avira URL Cloud	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
standoutglobal.com	162.240.9.126	true	false	• 3%, Virustotal, Browse	unknown
vendes.marketing	107.180.46.229	true	false	• 3%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://vendes.marketing/transmigrant/Wplzr/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.240.9.126	standoutglobal.com	United States		46606	UNIFIEDLAYER-AS-1US	false
107.180.46.229	vendes.marketing	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532474
Start date:	02.12.2021
Start time:	10:22:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SCAN_7295943480515097.xlsm
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:	22
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:	mal68.expl.winXLSM@3/7@2/2
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: .xlsm • 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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.240.9.126	SCAN_7295943480515097.xlsm	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
107.180.46.229	SCAN_7295943480515097.xlsm	Get hash	malicious	Browse	• vendes.marketing/transmigrant/Wplzr/
	Purchase Inquiry&Product Specification.exe	Get hash	malicious	Browse	• www.nihongo.school/cu6s/?u6utf=W50CE7q4q9oP7gRqIAd9YQ9RaMYKauZAxq11Ezs86ZRrs4WUxbwZ3395pe/S2qg7huHC&9rN46F=xVMHGdB8

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
vendes.marketing	SCAN_7295943480515097.xlsm	Get hash	malicious	Browse	• 107.180.46.229

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	SCAN_7295943480515097.xlsm	Get hash	malicious	Browse	• 162.240.9.126
	INVOICE.exe	Get hash	malicious	Browse	• 162.214.80.6
	img20048901738_Pago.pdf.exe	Get hash	malicious	Browse	• 192.185.115.3
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	• 162.241.126.156
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	• 162.241.126.156
	New order documents. pdf.....exe	Get hash	malicious	Browse	• 108.179.232.76
	part-1500645108.xlsb	Get hash	malicious	Browse	• 162.241.62.201
	img20048901740_Pago.pdf.exe	Get hash	malicious	Browse	• 192.185.115.3
	part-1500645108.xlsb	Get hash	malicious	Browse	• 162.241.62.201
	shedy.exe	Get hash	malicious	Browse	• 162.241.218.172
	product list.xlsx	Get hash	malicious	Browse	• 162.241.218.178
	accounts...exe	Get hash	malicious	Browse	• 192.185.164.148
	New product of Aluminium Profile.exe	Get hash	malicious	Browse	• 192.185.84.191
	BL. AWSMUNDAR3606-21.exe	Get hash	malicious	Browse	• 162.241.148.56
	draft_inv dec21.exe	Get hash	malicious	Browse	• 162.241.120.147
	bank details.exe	Get hash	malicious	Browse	• 192.185.134.38
	NEW INQUIRY ORDER.vbs	Get hash	malicious	Browse	• 192.185.29.73
	Details.exe	Get hash	malicious	Browse	• 192.185.164.148
	COMMERCIAL INVOICE AND BILL OF LANDING... 11232021.exe	Get hash	malicious	Browse	• 192.185.84.191
	counter-119221000.xls	Get hash	malicious	Browse	• 108.179.192.98
AS-26496-GO-DADDY-COM-LLCUS	SCAN_7295943480515097.xlsm	Get hash	malicious	Browse	• 107.180.46.229
	PAYMENT PROOF.exe	Get hash	malicious	Browse	• 160.153.63.160
	TT swift copy.exe	Get hash	malicious	Browse	• 148.66.138.249
	DHL DOCUMENT FOR #504.exe	Get hash	malicious	Browse	• 72.167.241.180
	Purchase order.exe	Get hash	malicious	Browse	• 148.66.138.249
	swift copy.exe	Get hash	malicious	Browse	• 160.153.63.160
	print_01.exe	Get hash	malicious	Browse	• 107.180.56.180
	New order.exe	Get hash	malicious	Browse	• 148.66.138.249
	PO_30-11-2021.xlsx	Get hash	malicious	Browse	• 166.62.110.60
	New order.exe	Get hash	malicious	Browse	• 148.66.138.249
	ORDEN DE COMPRA (2).exe	Get hash	malicious	Browse	• 107.180.88.78
	remitted payment.exe	Get hash	malicious	Browse	• 160.153.63.160
	ORDEN DE COMPRA (2).exe	Get hash	malicious	Browse	• 107.180.88.78
	ABONOF2201_exe.exe	Get hash	malicious	Browse	• 107.180.56.180
	request quotation.exe	Get hash	malicious	Browse	• 107.180.38.104
	Linux_amd64	Get hash	malicious	Browse	• 160.153.92.132
	cT69PbT3G6.exe	Get hash	malicious	Browse	• 107.180.51.79

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PURCHASED ORDER CONFIRMATION UGANDA.xlsx	Get hash	malicious	Browse	• 148.72.214.23
	swift copy.exe	Get hash	malicious	Browse	• 160.153.63.160
	New order.exe	Get hash	malicious	Browse	• 148.66.138.249

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Kqn63gUZFq.exe	Get hash	malicious	Browse	• 107.180.46.229
	837375615376.dll	Get hash	malicious	Browse	• 107.180.46.229
	NTS_eTaxInvoice 1-12-2021#U00b7pdf.exe	Get hash	malicious	Browse	• 107.180.46.229
	837375615376.dll	Get hash	malicious	Browse	• 107.180.46.229
	lzJWJgZhPc.exe	Get hash	malicious	Browse	• 107.180.46.229
	#U0420R#U04223445FM.htm	Get hash	malicious	Browse	• 107.180.46.229
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	• 107.180.46.229
	GlobalfoundriesINV33-45776648.htm	Get hash	malicious	Browse	• 107.180.46.229
	koCttsCjGY.exe	Get hash	malicious	Browse	• 107.180.46.229
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	• 107.180.46.229
	Chrome.Update.23af76.js	Get hash	malicious	Browse	• 107.180.46.229
	DHL Express shipment notification.exe	Get hash	malicious	Browse	• 107.180.46.229
	Chrome.Update.23af76.js	Get hash	malicious	Browse	• 107.180.46.229
	Transferencia_29_11_2021 17.03.39.exe	Get hash	malicious	Browse	• 107.180.46.229
	part-1500645108.xlsb	Get hash	malicious	Browse	• 107.180.46.229
	gXphSPTf52.exe	Get hash	malicious	Browse	• 107.180.46.229
	VM845.html	Get hash	malicious	Browse	• 107.180.46.229
	Rl3M5OSf6P.exe	Get hash	malicious	Browse	• 107.180.46.229
	#U0192#U0e25#U00a2_#U0192#U03b1#U0aee#U01ad#U00b5#U0ae8#U03b1_#U05e0jumozeK_Yim73678.vbs	Get hash	malicious	Browse	• 107.180.46.229
	DOC209272621615.PDF.exe	Get hash	malicious	Browse	• 107.180.46.229

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\7A7D450E-0610-43BD-BE93-0BD5327AEEE8	
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):	140193
Entropy (8bit):	5.357949437721391
Encrypted:	false
SSDEEP:	1536:NcQIfgxrBdA3gBwtnQ9DQW+z2k4Ff7nXbovidXiE6LWmE9:XuQ9DQW+zYXfH
MD5:	D8DEC9CBF6330B55B3306F1D12FAEC39
SHA1:	3423392A1DA9FFAD2FB1FD41A5A68196EFDAEECC
SHA-256:	1CAE713D69A6E3D907F5B5CB994E9ACBD858CFF49DBFFE3287E84C8000C789F6
SHA-512:	C636035796B7B4840C55FBC561D5D852712782BBBAB8368BBA662BE52CFD7DF1EB330A1E3D842E6D04B81B6B8D74F4A615821BDB517D4A116975B8CA399FBE4
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="2021-12-02T09:26:03">.. Build: 16.0.14715.30527-->.. <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\33AE098B.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\33AE098B.tmp	
Encrypted:	false
SSDEEP:	3:YmsalTlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB 9E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\DCF4C732.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 1714 x 241, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	14200
Entropy (8bit):	7.855440184003825
Encrypted:	false
SSDEEP:	384:aeN0UV6iAmjeSvWFL3SdwHEpS4Q24kc49+Tb:jmUxjfC30+kS4Qyob
MD5:	4FE798EE522800691796BC9446918C90
SHA1:	1E01CDE49D0B1B5E2F0DFBAD568DC2ECFBEDEAD3
SHA-256:	EC0BC049D3D30C29567806EB2D555589CD2E1B6B30E9145F77B73A32EC1C1087
SHA-512:	FF968DA2D921DA198E93E82E2FB15583CFA4696455755A6674BC321CD90AE5502ADDC445A0F8C630D9DC780E77EEC6FFC83F55CD2C16DDE7F465BFD0D89BF AA
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....-.....sRGB.....gAMA.....a.....PLTE....6...6.....6..a..a..6.....a.....a...aa....6....6...66666.6aa..a..6aaa...a....66.....aaaa..aaaa6a....a....66...6.a.....S.b..... 6.:...b....f....S.....t:...6t...f.....:6...S:6.:bS.....fbS..Sf.t.....:.t..t....bS..tfb..6.f...Sfb.....:.S.....6l...WtRNS.....c5.....pHYs... .....o.d..5.IDATx^.....q....R.A...[.I...'@. .....G..'..;...%..]U]3s....x.s.;.]]..W.....~..|...../~ ...?.{...~fe./...).H....Og1.6g....1T+v..'"h.._(Z;.Zh.bo.....rip..5.>..).h..(F....Z.[.q2B.WZz,...M}@..n$.dO.VK?.....YZ...."-o#.K..q..-#5.JT1.K.H..]se.M+.!...R..m{..Q#lO..^ev.R:...0 .>.....\....=.>.Op.<..p....qN.Vfq,..\F..6.1..+.. .J....c.4?.Jx...u..X+.E.D...Ko.}...s..G..8l.v...8'B....y..).

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\P0UY3TPH.htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	174739
Entropy (8bit):	5.2177771329382745
Encrypted:	false
SSDEEP:	3072:Ey/WQHnjZZ++99ffmmWWdmblJwNFmbxikGHSllanRYGUqcVudlxMu:Ey/WQHnjZZ++99ffmmWWdmbldbxs
MD5:	8390656A9CE7D214386AE81EA0B89D32
SHA1:	B2B0D4E1F626E16601C3F58EC95109A06312AEF7
SHA-256:	AC7541E64DD6B4FAF9E12E8DB314AFB68F2E35B8ADBE0EA87C2B5B2D879240A0
SHA-512:	95FC9DFAE57FD87B252DF9973955BB4DC3EDEB7048BA2B51C12C519F4BB31F223C0A3603F73B0A5558F352817726F89E8CEFC97C49AC1BC8D00A1122A8D00A B
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html lang="es">.<head>..<meta charset="UTF-8">..<meta name="viewport" content="width=device-width, initial-scale=1.0, viewport-fit=cover" />..< title>Agencia #1 de Marketing Digital en M.xico y La Mejor de LatinoAm.rica | Vendes.Marketing</title>.<meta name="dc.title" content="Agencia #1 de Marketing Digital en M.xico y La Mejor de LatinoAm.rica | Vendes.Marketing" />.<meta name="dc.description" content="La mejor agencia de especialistas en estrategias de marketing digital con enfoque en aumentar tus ventas r.pido. Asesor.a y acompa.amiento de profesionales para conseguir m.s clientes. Obt.n tu revisi.n de marketing digital GRATIS ahora !" />.<meta name="dc.relation" content="https://vendes.marketing/" />.<meta name="dc.source" content="https://vendes.marketing/" />.<meta name="dc.language" con tent="es_ES" />.<meta name="description" content="La mejor agencia de especialistas en estrategias de marketing digital con enfoque en aumentar tus ventas r.pido. Asesor

C:\Users\user\AppData\Local\Temp\~DFC9202BBA01CD114F.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B

C:\Users\user\AppData\Local\Temp\~DFC9202BBA01CD114F.TMP	
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 FE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.....

C:\Users\user\Desktop\~$SCAN_7295943480515097.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362 7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

C:\Users\user\besta.ocx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	174739
Entropy (8bit):	5.2177771329382745
Encrypted:	false
SSDEEP:	3072:Ey/WQHnjZZ++99ffmmWWdmblJwNFmbxikGHSllanRYGUqcVudlxMu:Ey/WQHnjZZ++99ffmmWWdmbldbxs
MD5:	8390656A9CE7D214386AE81EA0B89D32
SHA1:	B2B0D4E1F626E16601C3F58EC95109A06312AEF7
SHA-256:	AC7541E64DD6B4FAF9E12E8DB314AFB68F2E35B8ADBE0EA87C2B5B2D879240A0
SHA-512:	95FC9DFAE57FD87B252DF9973955BB4DC3EDEB7048BA2B51C12C519F4BB31F223C0A3603F73B0A5558F352817726F89E8CEFC97C49AC1BC8D00A1122A8D00A B
Malicious:	false
Preview:	<!DOCTYPE html>.<html lang="es">.<head>..<meta charset="UTF-8">..<meta name="viewport" content="width=device-width, initial-scale=1.0, viewport-fit=cover" />.. title>Agencia #1 de Marketing Digital en M.xico y La Mejor de LatinoAm.rica | Vendes.Marketing</title>.<meta name="dc.title" content="Agencia #1 de Marketing Digital en M.xico y La Mejor de LatinoAm.rica | Vendes.Marketing" />.<meta name="dc.description" content="La mejor agencia de especialistas en estrategias de marketing digital con enfoque en aumentar tus ventas r.pido. Asesor.a y acompa.amiento de profesionales para conseguir m.s clientes. Obt.n tu revisi.n de marketing digital GRATIS ahora !" />.<meta name="dc.relation" content="https://vendes.marketing/" />.<meta name="dc.source" content="https://vendes.marketing/" />.<meta name="dc.language" con tent="es_ES" />.<meta name="description" content="La mejor agencia de especialistas en estrategias de marketing digital con enfoque en aumentar tus ventas r.pido. Asesor

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.624498524713085
TrID:	• Excel Microsoft Office Open XML Format document with Macro (51004/1) 51.52% • Excel Microsoft Office Open XML Format document (40004/1) 40.40% • ZIP compressed archive (8000/1) 8.08%
File name:	SCAN_7295943480515097.xlsm
File size:	38040
MD5:	1ab11dce30326f39f6186f9aa05d5777
SHA1:	397dd88ca9d78a16ab549a8d22a711ddbea80c05
SHA256:	8f8e07b2eaca8af62e86cebd2372f1b85d420091801ec47 2796387a44a98bbcd

General

SHA512:	388f99c4621c31b2a696fa271b71a7ac0424bd1114054ee 1cf19d20883a25b31184b07b7bc31eb016876fc4163b4b3 ac21298c2c5cb9d1edb9e0560da32f9cd5
SSDEEP:	768:a/l83XfjrjevZCwVItvxmUxjfC30+kS4QyoO0VIqwgb: anrIItvxXYk4pTVIqR
File Content Preview:	PK.....!.L#li.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "SCAN_7295943480515097.xlsm"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 10:26:07.519718885 CET	192.168.2.3	8.8.8.8	0x12be	Standard query (0)	standoutglobal.com	A (IP address)	IN (0x0001)
Dec 2, 2021 10:27:30.134660959 CET	192.168.2.3	8.8.8.8	0x1f5	Standard query (0)	vendes.marketing	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 10:26:08.131093979 CET	8.8.8.8	192.168.2.3	0x12be	No error (0)	standoutglobal.com		162.240.9.126	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 10:27:30.154655933 CET	8.8.8.8	192.168.2.3	0x1f5	No error (0)	vendes.marketing		107.180.46.229	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- vendes.marketing
- standoutglobal.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49807	107.180.46.229	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49740	162.240.9.126	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 10:26:17.800939083 CET	1268	OUT	GET /2/MWpqeVgZ/ HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: standoutglobal.com Connection: Keep-Alive
Dec 2, 2021 10:26:20.813682079 CET	1268	OUT	GET /2/MWpqeVgZ/ HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: standoutglobal.com Connection: Keep-Alive
Dec 2, 2021 10:26:23.860819101 CET	1269	OUT	GET /2/MWpqeVgZ/ HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: standoutglobal.com Connection: Keep-Alive
Dec 2, 2021 10:26:29.861299038 CET	1292	OUT	GET /2/MWpqeVgZ/ HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: standoutglobal.com Connection: Keep-Alive
Dec 2, 2021 10:26:41.862371922 CET	1292	OUT	GET /2/MWpqeVgZ/ HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: standoutglobal.com Connection: Keep-Alive
Dec 2, 2021 10:26:53.863374949 CET	2076	OUT	GET /2/MWpqeVgZ/ HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: standoutglobal.com Connection: Keep-Alive
Dec 2, 2021 10:27:05.864382029 CET	2120	OUT	GET /2/MWpqeVgZ/ HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: standoutglobal.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 10:27:29.866477013 CET	9897	OUT	GET /2/MWpqeVgZ/ HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: standoutglobal.com Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49806	107.180.46.229	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 10:27:30.269488096 CET	9898	OUT	GET /transmigrant/Wplzr/ HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: vendes.marketing Connection: Keep-Alive
Dec 2, 2021 10:27:31.017816067 CET	9898	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 02 Dec 2021 09:27:30 GMT Server: Apache X-Powered-By: PHP/7.3.30 Link: <https://vendes.marketing/wp-json/>; rel="https://api.w.org/" Expires: Thu, 02 Dec 2021 10:27:30 GMT Cache-Control: max-age=3600 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Location: https://vendes.marketing Content-Length: 0 Keep-Alive: timeout=5 Content-Type: text/html; charset=UTF-8

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49807	107.180.46.229	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-12-02 09:27:31 UTC	0	OUT	GET / HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Connection: Keep-Alive Host: vendes.marketing
2021-12-02 09:27:32 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 09:27:31 GMT Server: Apache X-Powered-By: PHP/7.3.30 Link: <https://vendes.marketing/wp-json/>; rel="https://api.w.org/", <https://vendes.marketing/wp-json/wp/v2/pages/1522>; rel="alternate"; type="application/json", <https://vendes.marketing/>; rel=shortlink Set-Cookie: htmove_has_count-1522=htmovealreadycount; path=/ Upgrade: h2,h2c Connection: Upgrade, close Vary: Accept-Encoding Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2021-12-02 09:27:32 UTC	0	IN	Data Raw: 32 34 61 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 73 22 3e 0a 3c 68 65 61 64 3e 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 76 69 65 77 70 6f 72 74 2d 66 69 74 3d 63 6f 76 65 72 22 20 2f 3e 09 09 3c 74 69 74 6c 65 3e 41 67 65 6e 63 69 61 20 23 31 20 64 65 20 4d 61 72 6b 65 74 69 6e 67 20 44 69 67 69 74 61 6c 20 65 6e 20 4d c3 a9 78 69 63 6f 20 79 20 4c 61 20 4d 65 6a 6f 72 20 64 65 20 4c 61 74 69 6e 6f 41 6d c3 a9 72 69 63 61 20 7c 20 56 65 6e 64 65 73 2e 4d 61 Data Ascii: 24a3<!DOCTYPE html><html lang="es"><head><meta charset="UTF-8"><meta name="viewport" con tent="width=device-width, initial-scale=1.0, viewport-fit=cover" /><title>Agencia #1 de Marketing Digital en Mxico y La Mejor de LatinoAmrica | Vendes.Ma

Timestamp	kBytes transferred	Direction	Data
2021-12-02 09:27:32 UTC	8	IN	Data Raw: 6c 65 61 72 52 65 63 74 28 30 2c 30 2c 69 2e 77 69 64 74 68 2c 69 2e 68 65 69 67 68 74 29 2c 70 2e 66 69 6c 6c 54 65 78 74 28 61 2e 61 70 70 6c 79 28 74 68 69 73 2c 65 29 2c 30 2c 30 29 3b 65 3d 69 2e 74 6f 44 61 74 61 55 52 4c 28 29 3b 72 65 74 75 72 6e 20 70 2e 63 6c 65 61 72 52 65 63 74 28 30 2c 30 2c 69 2e 77 69 64 74 68 2c 69 2e 68 65 69 67 68 74 29 2c 70 2e 66 69 6c 6c 54 65 78 74 28 61 2e 61 70 70 6c 79 28 74 68 69 73 2c 74 29 2c 30 2c 30 29 2c 65 3d 3d 3d 69 2e 74 6f 44 61 74 61 55 52 4c 28 29 7d 66 75 6e 63 74 69 6f 6e 20 63 28 65 29 7b 76 61 72 20 74 3d 61 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 74 2e 73 72 63 3d 65 2c 74 2e 64 65 66 65 72 3d 74 2e 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 Data Ascii: learRect(0,0,i.width,i.height),p.fillText(a.apply(this,e),0,0);e=i.toDataURL();return p.clearRect(0,0,i.width,i.height),p.fillText(a.apply(this,t),0,0),e===i.toDataURL()}function c(e){var t=a.createElement("script");t.src=e,t.defer=t.type="text/javascript
2021-12-02 09:27:32 UTC	9	IN	Data Raw: 0d 0a Data Ascii:
2021-12-02 09:27:32 UTC	9	IN	Data Raw: 34 30 30 30 0d 0a 3c 73 74 79 6c 65 3e 0a 69 6d 67 2e 77 70 2d 73 6d 69 6c 65 79 2c 0a 69 6d 67 2e 65 6d 6f 6a 69 20 7b 0a 09 64 69 73 70 6c 61 79 3a 20 69 6e 6c 69 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 0a 09 62 6f 72 64 65 72 3a 20 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 0a 09 62 6f 78 2d 73 68 61 64 6f 77 3a 20 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 0a 09 68 65 69 67 68 74 3a 20 31 65 6d 20 21 69 6d 70 6f 72 74 61 6e 74 3b 0a 09 77 69 64 74 68 3a 20 31 65 6d 20 21 69 6d 70 6f 72 74 61 6e 74 3b 0a 09 6d 61 72 67 69 6e 3a 20 30 20 2e 30 37 65 6d 20 21 69 6d 70 6f 72 74 61 6e 74 3b 0a 09 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 20 2d 30 2e 31 65 6d 20 21 69 6d 70 6f 72 74 61 6e 74 3b 0a 09 62 61 63 6b 67 72 6f 75 6e 64 3a 20 6e 6f Data Ascii: 4000<style>img.wp-smiley,img.emoji {display: inline !important;border: none !important;box-shadow: none !important;height: 1em !important;width: 1em !important;margin: 0 .07em !important;vertical-align: -0.1em !important;background: no
2021-12-02 09:27:32 UTC	17	IN	Data Raw: 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 73 63 61 6c 65 33 64 28 2e 39 37 2c 2e 39 37 2c 2e 39 37 29 3b 74 72 61 6e 73 66 6f 72 6d 3a 73 63 61 6c 65 33 64 28 2e 39 37 2c 2e 39 37 2c 2e 39 37 29 7d 74 6f 7b 6f 70 61 63 69 74 79 3a 31 7d 7d 40 6b 65 79 66 72 61 6d 65 73 20 68 61 5f 62 6f 75 6e 63 65 49 6e 7b 30 25 2c 32 30 25 2c 34 30 25 2c 36 30 25 2c 38 30 25 2c 74 6f 7b 2d 77 65 62 6b 69 74 2d 61 6e 69 6d 61 74 69 6f 6e 2d 74 69 6d 69 6e 67 2d 66 75 6e 63 74 69 6f 6e 3a 63 75 62 69 63 2d 62 65 7a 69 65 72 28 2e 32 31 35 2c 2e 36 31 2c 2e 33 35 35 2c 31 29 3b 61 6e 69 6d 61 74 69 6f 6e 2d 74 69 6d 69 6e 67 2d 66 75 6e 63 74 69 6f 6e 3a 63 75 62 69 63 2d 62 65 7a 69 65 72 28 2e 32 31 35 2c 2e 36 31 2c 2e 33 35 35 2c 31 29 7d 30 25 7b 6f 70 61 63 69 Data Ascii: ebkit-transform:scale3d(.97,.97,.97);transform:scale3d(.97,.97,.97)}to{opacity:1}}@keyframes ha_bounceIn{0%,20%,40%,60%,80%,to{-webkit-animation-timing-function:cubic-bezier(.215,.61,.355,1);animation-timing-function:cubic-bezier(.215,.61,.355,1)}0%{opaci
2021-12-02 09:27:32 UTC	25	IN	Data Raw: 0d 0a Data Ascii:
2021-12-02 09:27:32 UTC	25	IN	Data Raw: 31 62 34 62 0d 0a 69 6d 67 7b 6d 61 78 2d 77 69 64 74 68 3a 31 30 30 25 3b 68 65 69 67 68 74 3a 61 75 74 6f 3b 2d 6f 2d 6f 62 6a 65 63 74 2d 66 69 74 3a 63 6f 76 65 72 3b 6f 62 6a 65 63 74 2d 66 69 74 3a 63 6f 76 65 72 7d 2e 68 61 2d 73 63 72 65 65 6e 2d 72 65 61 64 65 72 2d 74 65 78 74 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 3b 63 6c 69 70 3a 72 65 63 74 28 31 70 78 2c 31 70 78 2c 31 70 78 29 3b 6d 61 72 67 69 6e 3a 2d 31 70 78 3b 70 61 64 64 69 6e 67 3a 30 3b 77 69 64 74 68 3a 31 70 78 3b 68 65 69 67 68 74 3a 31 70 78 3b 62 6f 72 64 65 72 3a 30 3b 77 6f 72 64 2d 77 72 61 70 3a 6e 6f 72 6d 61 6c 21 69 6d 70 6f 72 74 61 6e 74 3b 2d 77 65 62 6b 69 74 2d 63 6c 69 70 2d 70 61 74 68 3a Data Ascii: 1b4bimg{max-width:100%;height:auto;-o-object-fit:cover;object-fit:cover}.ha-screen-reader-text{position:absolute;overflow:hidden;clip:rect(1px,1px,1px,1px);margin:-1px;padding:0;width:1px;height:1px;border:0;word-wrap:normal!important;-webkit-clip-path:
2021-12-02 09:27:32 UTC	33	IN	Data Raw: 61 70 70 79 2d 69 63 6f 6e 73 2d 63 73 73 27 20 20 68 72 65 66 3d 27 68 74 74 70 73 3a 2f 2f 76 65 6e 64 65 73 2e 6d 61 72 6b 65 74 69 6e 67 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 68 61 70 70 79 2d 65 6c 65 6d 65 6e 74 6f 72 2d 61 64 64 6f 6e 73 2f 61 73 73 65 74 73 2f 66 6f 6e 74 73 2f 73 74 79 6c 65 2e 6d 69 6e 2e 63 73 73 3f 76 65 72 3d 33 2e 33 2e 30 27 20 6d 65 64 69 61 3d 27 61 6c 6c 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 27 73 74 79 6c 65 73 68 65 65 74 27 20 69 64 3d 27 66 6f 6e 74 2d 61 77 65 73 6f 6d 65 2d 63 73 73 27 20 20 68 72 65 66 3d 27 68 74 74 70 73 3a 2f 2f 76 65 6e 64 65 73 2e 6d 61 72 6b 65 74 69 6e 67 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 65 6c 65 6d 65 6e 74 6f 72 2f 61 73 73 65 74 73 Data Ascii: appy-icons-css' href='https://vendes.marketing/wp-content/plugins/happy-elementor-addons/assets/fonts/style.min.css?ver=3.3.0' media='all' /><link rel='stylesheet' id='font-awesome-css' href='https://vendes.marketing/wp-content/plugins/elementor/assets
2021-12-02 09:27:32 UTC	48	IN	Data Raw: 0d 0a Data Ascii:
2021-12-02 09:27:32 UTC	48	IN	Data Raw: 34 30 30 30 0d 0a 64 69 73 65 6e 6f 2d 65 64 69 74 6f 72 69 61 6c 2f 22 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 73 75 62 2d 69 74 65 6d 22 3e 44 69 73 65 c3 b1 6f 20 45 64 69 74 6f 72 69 61 6c 3c 2f 61 3e 3c 2f 6c 69 3e 0a 09 3c 6c 69 20 63 6c 61 73 73 3d 22 6d 65 6e 75 2d 69 74 65 6d 20 6d 65 6e 75 2d 69 74 65 6d 2d 74 79 70 65 2d 70 6f 73 74 5f 74 79 70 65 20 6d 65 6e 75 2d 69 74 65 6d 2d 6f 62 6a 65 63 74 2d 70 61 67 65 20 6d 65 6e 75 2d 69 74 65 6d 2d 69 74 65 6d 2d 32 30 34 36 22 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 76 65 6e 64 65 73 2e 6d 61 72 6b 65 74 69 6e 67 2f 61 67 65 6e 63 69 61 2d 64 65 2d 6d 61 72 6b 65 74 69 6e 67 2d 64 69 67 69 74 61 6c 2f 73 65 72 76 69 63 69 6f 73 2d 63 72 65 61 74 69 76 6f 73 2f 64 69 73 65 6e 6f 2d 77 Data Ascii: 4000diseno-editorial/" class="elementor-sub-item">Diseo Editorial <li class="menu-item menu-item-type-post_type menu-item-object-page menu-item-2046"><a href="https://vendes.marketing/agencia-de-marketing-digital/servicios-creativos/diseno-w
2021-12-02 09:27:32 UTC	56	IN	Data Raw: 65 6e 75 2d 69 74 65 6d 20 6d 65 6e 75 2d 69 74 65 6d 2d 74 79 70 65 2d 70 6f 73 74 5f 74 79 70 65 20 6d 65 6e 75 2d 69 74 65 6d 2d 6f 62 6a 65 63 74 2d 70 61 67 65 20 6d 65 6e 75 2d 69 74 65 6d 2d 32 32 33 38 22 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 76 65 6e 64 65 73 2e 6d 61 72 6b 65 74 69 6e 67 2f 61 67 65 6e 63 69 61 2d 64 65 2d 6d 61 72 6b 65 74 69 6e 67 2d 64 69 67 69 74 61 6c 2f 63 6f 6e 73 6c 74 6f 72 69 61 73 2f 63 6f 6e 73 75 6c 74 6f 72 69 61 2d 70 61 72 61 2d 61 64 73 65 6e 73 65 2f 22 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 73 75 62 2d 69 74 65 6d 22 3e 43 6f 6e 73 75 6c 74 6f 72 c3 ad 61 20 70 61 72 61 20 41 64 53 65 6e 73 65 3c 2f 61 3e 3c 2f 6c 69 3e 0a 09 3c 6c 69 20 63 6c 61 73 73 3d 22 6d 65 6e 75 2d 69 Data Ascii: enu-item menu-item-type-post_type menu-item-object-page menu-item-2238">Consultora para AdSense <li class="menu-i
2021-12-02 09:27:32 UTC	64	IN	Data Raw: 0d 0a Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2021-12-02 09:27:32 UTC	64	IN	Data Raw: 32 37 35 62 0d 0a 2d 74 79 70 65 2d 70 6f 73 74 5f 74 79 70 65 20 6d 65 6e 75 2d 69 74 65 6d 2d 6f 62 6a 65 63 74 2d 70 61 67 65 20 6d 65 6e 75 2d 69 74 65 6d 2d 32 30 34 38 22 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 76 65 6e 64 65 73 2e 6d 61 72 6b 65 74 69 6e 67 2f 61 67 65 6e 63 69 61 2d 64 65 2d 6d 61 72 6b 65 74 69 6e 67 2d 64 69 67 69 74 61 6c 2f 73 65 72 76 69 63 69 6f 73 2d 63 72 65 61 74 69 76 6f 73 2f 70 72 6f 64 75 63 63 69 6f 6e 2d 61 75 64 69 6f 76 69 73 75 61 6c 2f 22 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 73 75 62 2d 69 74 65 6d 22 3e 50 72 6f 64 75 63 63 69 c3 b3 6e 20 41 75 64 69 6f 76 69 73 75 61 6c 3c 2f 61 3e 3c 2f 6c 69 3e 0a 3c 2f 75 6c 3e 0a 3c 2f 6c 69 3e 0a 3c 6c 69 20 63 6c 61 73 73 3d 22 6d 65 6e 75 Data Ascii: 275b-type-post_type menu-item-object-page menu-item-2048">Produccin Audiovisual <li class="menu
2021-12-02 09:27:32 UTC	72	IN	Data Raw: 6e 64 65 73 2e 6d 61 72 6b 65 74 69 6e 67 2f 61 67 65 6e 63 69 61 2d 64 65 2d 6d 61 72 6b 65 74 69 6e 67 2d 64 69 67 69 74 61 6c 2f 63 6f 6e 73 75 6c 74 6f 72 69 61 73 2f 63 6f 6e 73 75 6c 74 6f 72 69 61 2d 65 6e 2d 6d 61 72 6b 65 74 69 6e 67 2d 62 61 73 61 64 6f 2d 65 6e 2d 70 65 72 66 6f 72 6d 61 6e 63 65 2f 22 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 73 75 62 2d 69 74 65 6d 22 3e 43 6f 6e 73 75 6c 74 6f 72 c3 ad 61 20 65 6e 20 4d 61 72 6b 65 74 69 6e 67 20 62 61 73 61 64 6f 20 65 6e 20 50 65 72 66 6f 72 6d 61 6e 63 65 3c 2f 61 3e 3c 2f 6c 69 3e 0a 09 3c 6c 69 20 63 6c 61 73 73 3d 22 6d 65 6e 75 2d 69 74 65 6d 20 6d 65 6e 75 2d 69 74 65 6d 2d 74 79 70 65 2d 70 6f 73 74 5f 74 79 70 65 20 6d 65 6e 75 2d 69 74 65 6d 2d 6f 62 6a 65 63 74 2d 70 Data Ascii: ndes.marketing/agencia-de-marketing-digital/consultorias/consultoria-en-marketing-basado-en-performance/" class="elementor-sub-item">Consultora en Marketing basado en Performance <li class="menu-item menu-item-type-post_type menu-item-object-p
2021-12-02 09:27:32 UTC	74	IN	Data Raw: 0d 0a Data Ascii:
2021-12-02 09:27:32 UTC	74	IN	Data Raw: 34 30 30 30 0d 0a 09 09 3c 64 69 76 20 64 61 74 61 2d 65 6c 65 6d 65 6e 74 6f 72 2d 74 79 70 65 3d 22 77 70 2d 70 61 67 65 22 20 64 61 74 61 2d 65 6c 65 6d 65 6e 74 6f 72 2d 69 64 3d 22 31 35 32 32 22 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 20 65 6c 65 6d 65 6e 74 6f 72 2d 31 35 32 32 22 20 64 61 74 61 2d 65 6c 65 6d 65 6e 74 6f 72 2d 73 65 74 74 69 6e 67 73 3d 22 5b 5d 22 3e 0a 09 09 09 09 09 09 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 73 65 63 74 69 6f 6e 2d 77 72 61 70 22 3e 0a 09 09 09 09 09 09 09 3c 73 65 63 74 69 6f 6e 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 73 65 63 74 69 6f 6e 20 65 6c 65 6d 65 6e 74 6f 72 2d 74 6f 70 2d 73 65 63 74 69 6f 6e 20 65 6c 65 6d 65 6e 74 Data Ascii: 4000 <section class="elementor-section elementor-top-section elementor-element
2021-12-02 09:27:32 UTC	82	IN	Data Raw: 6d 65 6e 74 20 65 6c 65 6d 65 6e 74 6f 72 2d 65 6c 65 6d 65 6e 74 2d 65 62 38 36 34 31 61 20 65 6c 65 6d 65 6e 74 6f 72 2d 69 63 6f 6e 2d 6c 69 73 74 2d 2d 6c 61 79 6f 75 74 2d 69 6e 6c 69 6e 65 20 65 6c 65 6d 65 6e 74 6f 72 2d 61 6c 69 67 6e 2d 63 65 6e 74 65 72 20 65 6c 65 6d 65 6e 74 6f 72 2d 6c 69 73 74 2d 69 74 65 6d 2d 6c 69 6e 6b 2d 66 75 6c 6c 5f 77 69 64 74 68 20 65 6c 65 6d 65 6e 74 6f 72 2d 77 69 64 67 65 74 20 65 6c 65 6d 65 6e 74 6f 72 2d 77 69 64 67 65 74 2d 69 63 6f 6e 2d 6c 69 73 74 22 20 64 61 74 61 2d 69 64 3d 22 65 62 38 36 34 31 61 22 20 64 61 74 61 2d 65 6c 65 6d 65 6e 74 5f 74 79 70 65 3d 22 77 69 64 67 65 74 22 20 64 61 74 61 2d 77 69 64 67 65 74 5f 74 79 70 65 3d 22 6 9 63 6f 6e 2d 6c 69 73 74 2e 64 65 66 61 75 6c 74 22 3e 0a 09 09 Data Ascii: ment elementor-element-eb8641a elementor-icon-list--layout-inline elementor-align-center elementor-list-item-link-full_width elementor-widget elementor-widget-icon-list" data-id="eb8641a" data-element_type="widget" data-widget_type="icon-list.default">
2021-12-02 09:27:32 UTC	90	IN	Data Raw: 0d 0a Data Ascii:
2021-12-02 09:27:32 UTC	90	IN	Data Raw: 34 30 30 30 0d 0a 09 09 09 09 09 09 09 09 09 09 09 09 09 09 3c 69 6d 67 20 77 69 64 74 68 3d 22 36 36 32 22 20 68 65 69 67 68 74 3d 22 35 39 35 22 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 76 65 6e 64 65 73 2e 6d 61 72 6b 65 74 69 6e 67 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 75 70 6c 6f 61 64 73 2f 32 30 32 31 2f 31 30 2f 61 6e 75 6e 63 69 6f 73 2e 70 6e 67 22 20 63 6c 61 73 73 3d 22 61 74 74 61 63 68 6d 65 6e 74 2d 66 75 6c 6c 20 73 69 7a 65 2d 66 75 6c 6c 22 20 61 6c 74 3d 22 22 20 6c 6f 61 64 69 6e 67 3d 22 6c 61 7a 79 22 20 73 72 63 73 65 74 3d 22 68 74 74 70 73 3a 2f 2f 76 65 6e 64 65 73 2e 6d 61 72 6b 65 74 69 6e 67 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 75 70 6c 6f 61 64 73 2f 32 30 32 31 2f 31 30 2f 61 6e 75 6e 63 69 6f 73 2e 70 6e 67 20 36 36 32 77 Data Ascii: 4000<img width="662" height="595" src="https://vendes.marketing/wp-content/uploads/2021/10/anuncios.png" class="attachment-full size-full" alt="" loading="lazy" srcset="https://vendes.marketing/wp-content/uploads/2021/10/anuncios.png 662w
2021-12-02 09:27:32 UTC	98	IN	Data Raw: 77 69 64 67 65 74 2d 77 72 61 70 20 65 6c 65 6d 65 6e 74 6f 72 2d 65 6c 65 6d 65 6e 74 2d 70 6f 70 75 6c 61 74 65 64 22 3e 0a 09 09 09 09 09 09 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 65 6c 65 6d 65 6e 74 20 65 6c 65 6d 65 6e 74 6f 72 2d 65 6c 65 6d 65 6e 74 2d 30 61 38 31 31 36 38 20 65 6c 65 6d 65 6e 74 6f 72 2d 77 69 64 67 65 74 20 65 6c 65 6d 65 6e 74 6f 72 2d 77 69 64 67 65 74 2d 68 74 6d 6c 22 20 64 61 74 61 2d 69 64 3d 22 30 61 38 31 31 36 38 22 20 64 61 74 61 2d 65 6c 65 6d 65 6e 74 5f 74 79 70 65 3d 22 77 69 64 67 65 74 22 20 69 64 3 d 22 63 65 6e 74 65 72 22 20 64 61 74 61 2d 77 69 64 67 65 74 5f 74 79 70 65 3d 22 68 74 6d 6c 2e 64 65 66 61 75 6c 74 22 3e 0a 09 09 09 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 6c 65 Data Ascii: widget-wrap elementor-element-populated"> <div class="ele
2021-12-02 09:27:32 UTC	106	IN	Data Raw: 0d 0a Data Ascii:
2021-12-02 09:27:32 UTC	106	IN	Data Raw: 34 30 30 30 0d 0a 62 70 61 6e 65 6c 22 20 61 72 69 61 2d 6c 61 62 65 6c 6c 65 64 62 79 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 74 61 62 2d 74 69 74 6c 65 2d 37 35 33 31 22 3e 3c 70 3e 54 65 6e 65 6d 6f 73 20 70 6c 61 6e 65 73 20 64 65 73 64 65 20 3c 73 74 72 6f 6e 67 3e 24 39 39 55 53 44 3c 2f 73 74 72 6f 6e 67 3e 20 70 61 72 61 20 67 65 6e 65 72 61 72 20 63 6f 6e 74 65 6e 69 64 6f 20 65 6e 20 72 65 64 65 73 20 73 6f 63 69 61 6c 65 73 2e 3c 2f 70 3e 3c 2f 64 69 76 3e 0a 09 09 09 09 3c 2f 64 69 76 3e 0a 09 09 09 09 09 09 09 09 09 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6c 64 2b 6a 73 6f 6e 22 3e 7b 22 40 63 6f 6e 74 65 78 74 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 73 63 68 65 6d 61 2e 6f 72 67 22 2c 22 40 74 79 70 65 22 Data Ascii: 4000bpanel" aria-labelledby="elementor-tab-title-7531"> Tenemos planes desde $99USD para generar contenido en redes sociales. <script type="application/ld+json">{"@context":"https:\/\/ schema.org","@type"

Timestamp	kBytes transferred	Direction	Data
2021-12-02 09:27:32 UTC	114	IN	Data Raw: 6e 22 20 64 61 74 61 2d 69 64 3d 22 61 30 64 30 35 36 65 22 20 64 61 74 61 2d 65 6c 65 6d 65 6e 74 5f 74 79 70 65 3d 22 77 69 64 67 65 74 22 20 64 61 74 61 2d 77 69 64 67 65 74 5f 74 79 70 65 3d 22 62 75 74 74 6f 6e 2e 64 65 66 61 75 6c 74 22 3e 0a 09 09 09 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 77 69 64 67 65 74 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 0a 09 09 09 09 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 62 75 74 74 6f 6e 2d 77 72 61 70 70 65 72 22 3e 0a 09 09 09 3c 61 20 68 72 65 66 3d 22 23 70 6c 61 6e 65 73 2d 79 2d 70 72 65 63 69 6f 73 22 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 62 75 74 74 6f 6e 20 65 6c 65 6d 65 6e 74 6f 72 2d 62 75 74 74 6f 6e 2d 6c 69 6e 6b 20 65 6c 65 6d 65 6e 74 6f 72 2d 62 75 74 74 6f 6e 20 65 6c 65 6d 65 6e Data Ascii: n" data-id="a0d056e" data-element_type="widget" data-widget_type="button.default"> <a href="#planes-y-precios" class="elementor-button-link elementor-button elemen
2021-12-02 09:27:32 UTC	122	IN	Data Raw: 0d 0a Data Ascii:
2021-12-02 09:27:32 UTC	122	IN	Data Raw: 34 30 30 30 0d 0a 72 2d 74 61 62 2d 63 6f 6e 74 65 6e 74 20 65 6c 65 6d 65 6e 74 6f 72 2d 63 6c 65 61 72 66 69 78 22 20 64 61 74 61 2d 74 61 62 3d 22 31 22 20 72 6f 6c 65 3d 22 74 61 62 70 61 6e 65 6c 22 20 61 72 69 61 2d 6c 61 62 65 6c 6c 65 64 62 79 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 74 61 62 2d 74 69 74 6c 65 2d 32 33 32 31 22 3e 3c 70 3e 41 70 6f 72 74 61 20 65 6c 20 6d 61 79 6f 72 20 61 6c 63 61 6e 63 65 20 61 20 74 75 73 20 67 72 61 6e 64 65 73 20 70 72 6f 79 65 63 74 6f 73 20 65 6e 20 6c 61 20 77 65 62 2e 20 3c 61 20 68 72 65 66 3d 22 23 66 6f 72 6d 22 3e 53 6f 6c 69 63 69 74 61 20 75 6e 61 20 61 73 65 73 6f 72 c3 ad 61 3c 2f 61 3e 3c 2f 70 3e 3c 2f 64 69 76 3e 0a 09 09 09 09 3c 2f 64 69 76 3e 0a 09 09 09 09 09 09 09 09 09 3c 73 63 72 69 70 74 Data Ascii: 4000r-tab-content elementor-clearfix" data-tab="1" role="tabpanel" aria-labelledby="elementor-tab-title-2321"> Aporta el mayor alcance a tus grandes proyectos en la web. Solicita una asesora <script
2021-12-02 09:27:32 UTC	130	IN	Data Raw: 0a 09 09 09 09 09 09 09 09 09 3c 2f 6c 69 3e 0a 09 09 09 09 09 09 09 3c 6c 69 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 69 63 6f 6e 2d 6c 69 73 74 2d 69 74 65 6d 22 3e 0a 09 09 09 09 09 09 09 09 09 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 76 65 6e 64 65 73 2e 6d 61 72 6b 65 74 69 6e 67 2f 61 67 65 6e 63 69 61 2d 64 65 2d 6d 61 72 6b 65 74 69 6e 67 2d 64 69 67 69 74 61 6c 2f 65 2d 63 6f 6d 6d 65 72 63 65 2d 65 66 65 63 74 69 76 6f 2f 74 69 65 6e 64 61 2d 6f 6e 6c 69 6e 65 2d 63 6f 6e 2d 6d 61 67 65 6e 74 6f 2f 22 3e 0a 0a 09 09 09 09 09 09 09 09 09 09 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 69 63 6f 6e 2d 6c 69 73 74 2d 69 63 6f 6e 22 3e 0a 09 09 09 09 09 09 3c 69 20 61 72 69 61 2d 68 69 Data Ascii: <li class="elementor-icon-list-item"><a href="https://vendes.marketing/agencia-de-marketing-digital/e-commerce-efectivo/tienda-online-con-magento/"><i aria-hi
2021-12-02 09:27:32 UTC	138	IN	Data Raw: 0d 0a Data Ascii:
2021-12-02 09:27:33 UTC	138	IN	Data Raw: 33 62 34 35 0d 0a 61 74 65 64 22 3e 0a 09 09 09 09 09 09 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 65 6c 65 6d 65 6e 74 20 65 6c 65 6d 65 6e 74 6f 72 2d 65 6c 65 6d 65 6e 74 2d 63 38 35 62 39 38 65 20 65 6c 65 6d 65 6e 74 6f 72 2d 77 69 64 67 65 74 20 65 6c 65 6d 65 6e 74 6f 72 2d 77 69 64 67 65 74 2d 73 70 61 63 65 72 22 20 64 61 74 61 2d 69 64 3d 22 63 38 35 62 39 38 65 22 20 64 61 74 61 2d 65 6c 65 6d 65 6e 74 5f 74 79 70 65 3d 22 77 69 64 67 65 74 22 20 64 61 74 61 2d 77 69 64 67 65 74 5f 74 79 70 65 3d 22 73 70 61 63 65 72 2e 64 65 66 61 75 6c 74 22 3e 0a 09 09 09 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 77 69 64 67 65 74 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 0a 09 09 09 09 3c 64 69 76 20 63 Data Ascii: 3b45ated"> <div c
2021-12-02 09:27:33 UTC	146	IN	Data Raw: 65 6c 65 6d 65 6e 74 6f 72 2d 63 6f 6c 2d 31 30 30 20 65 6c 65 6d 65 6e 74 6f 72 2d 74 6f 70 2d 63 6f 6c 75 6d 6e 20 65 6c 65 6d 65 6e 74 6f 72 2d 65 6c 65 6d 65 6e 74 20 65 6c 65 6d 65 6e 74 6f 72 2d 65 6c 65 6d 65 6e 74 2d 63 36 36 65 37 32 63 22 20 64 61 74 61 2d 65 6c 65 6d 65 6e 74 5f 74 79 70 65 3d 22 63 6f 6c 75 6d 6e 22 3e 0a 09 09 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 77 69 64 67 65 74 2d 77 72 61 70 20 65 6c 65 6d 65 6e 74 6f 72 2d 65 6c 65 6d 65 6e 74 2d 70 6f 70 75 6c 61 74 65 64 22 3e 0a 09 09 09 09 09 09 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 65 6c 65 6d 65 6e 74 20 65 6c 65 6d 65 6e 74 6f 72 2d 65 6c 65 6d 65 6e 74 2d 62 38 Data Ascii: elementor-col-100 elementor-top-column elementor-element elementor-element-c66e72c" data-id="c66e72c" data-element_type="column"> <div class="elementor-element elementor-element-b8
2021-12-02 09:27:33 UTC	153	IN	Data Raw: 0d 0a Data Ascii:
2021-12-02 09:27:33 UTC	153	IN	Data Raw: 32 61 38 32 0d 0a 09 09 3c 64 69 76 20 64 61 74 61 2d 65 6c 65 6d 65 6e 74 6f 72 2d 74 79 70 65 3d 22 66 6f 6f 74 65 72 22 20 64 61 74 61 2d 65 6c 65 6d 65 6e 74 6f 72 2d 69 64 3d 22 32 31 35 37 22 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 20 65 6c 65 6d 65 6e 74 6f 72 2d 32 31 35 37 20 65 6c 65 6d 65 6e 74 6f 72 2d 6c 6f 63 61 74 69 6f 6e 2d 66 6f 6f 74 65 72 22 20 64 61 74 61 2d 65 6c 65 6d 65 6e 74 6f 72 2d 73 65 74 74 69 6e 67 73 3d 22 5b 5d 22 3e 0a 09 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 73 65 63 74 69 6f 6e 2d 77 72 61 70 22 3e 0a 09 09 09 09 3c 73 65 63 74 69 6f 6e 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 73 65 63 74 69 6f 6e 20 65 6c 65 6d 65 6e 74 6f 72 2d 74 6f 70 2d 73 65 63 74 69 6f 6e Data Ascii: 2a82 <section class="elementor-section elementor-top-section
2021-12-02 09:27:33 UTC	161	IN	Data Raw: 64 61 74 61 2d 65 6c 65 6d 65 6e 74 5f 74 79 70 65 3d 22 63 6f 6c 75 6d 6e 22 3e 0a 09 09 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 77 69 64 67 65 74 2d 77 72 61 70 20 65 6c 65 6d 65 6e 74 6f 72 2d 65 6c 65 6d 65 6e 74 2d 70 6f 70 75 6c 61 74 65 64 22 3e 0a 09 09 09 09 09 09 09 09 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 6c 65 6d 65 6e 74 6f 72 2d 65 6c 65 6d 65 6e 74 20 65 6c 65 6d 65 6e 74 6f 72 2d 65 6c 65 6d 65 6e 74 2d 34 37 30 62 32 30 34 31 20 65 6c 65 6d 65 6e 74 6f 72 2d 77 69 64 67 65 74 20 65 6c 65 6d 65 6e 74 6f 72 2d 77 69 64 67 65 74 2d 6d 65 6e 75 2d 61 6e 63 68 6f 72 22 20 64 61 74 61 2d 69 64 3d 22 34 37 30 62 32 30 34 31 22 20 64 61 74 61 2d 65 6c 65 6d 65 6e 74 5f 74 79 70 65 3d 22 77 69 64 67 65 74 22 20 64 61 Data Ascii: data-element_type="column"> <div class="elementor-element elementor-element-470b2041 elementor-widget elementor-widget-menu-anchor" data-id="470b2041" data-element_type="widget" da
2021-12-02 09:27:33 UTC	164	IN	Data Raw: 0d 0a Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2021-12-02 09:27:33 UTC	164	IN	Data Raw: 31 64 38 33 0d 0a 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 77 6f 6f 63 6f 6d 6d 65 72 63 65 20 68 74 6d 6f 76 65 2d 71 75 69 63 6b 2d 76 69 65 77 2d 6d 6f 64 61 6c 22 20 69 64 3d 22 68 74 6d 6f 76 65 71 75 69 63 6b 2d 76 69 65 77 6d 6f 64 61 6c 22 20 73 74 79 6c 65 3d 22 76 69 73 69 62 69 6c 69 74 79 3a 20 68 69 64 64 65 6e 3b 6f 70 61 63 69 74 79 3a 20 30 3b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 3b 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 68 74 6d 6f 76 65 2d 6d 6f 64 61 6c 2d 64 69 61 6c 6f 67 20 70 72 6f 64 75 63 74 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 68 74 6d 6f 76 65 2d 6d 6f 64 61 6c 2d 63 6f 6e 74 65 6e 74 22 3e 3c 62 75 74 74 6f 6e 20 74 79 70 65 3d 22 62 75 74 74 6f 6e 22 20 63 6c 61 73 73 3d 22 68 74 6d 6f 76 65 2d 6d 6f 64 61 6c 2d 63 6c 6f Data Ascii: 1d83 <button type="button" class="htmove-modal-clo

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 5980 Parent PID: 744

General

Start time:	10:26:01
Start date:	02/12/2021
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:	0xab0000
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 Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: rundll32.exe PID: 3928 Parent PID: 5980

General

Start time:	10:27:33
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWow64\rundll32.exe ..\besta.ocx,44532.4348061343
Imagebase:	0xc30000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Disassembly

Code Analysis