Detecting Possible Fraud Vehicles Specific to Latin America and the Caribbean

Table of Contents

Executive Report

Although fraud is a global issue, some threats may be unique to certain regions. Accertify listed some subtrends specific to Latin America and the Caribbean (LAC), including those involving the airline and digital wallet industries.

WhoisXML API researchers looked into these LAC-specific fraud trends and found:

- 4,500+ cybersquatting domains targeting LAC-based airlines
- 5,000+ cybersquatting domains targeting popular LAC-based digital wallet providers
- Less than 1% of the cybersquatting domains in both industries that could be publicly attributed to the imitated companies
- Several cybersquatting domains that were found malicious, with some hosting phishing content
- A public registrant email address used to register one of the malicious domains that led to a network comprising 60 domains, several of which were also found malicious and imitated well-known companies

Identifying Possible Fraud Vehicles

When Interpol described how airline ticket fraud works, the organization talked about cybercriminals using professional-looking websites as fronts for selling plane tickets. These tickets were bought using stolen or hacked credit cards and then offered for sale via professional-looking websites at reduced prices. While victims might think they found a great deal, they might eventually lose their tickets and money instead.

Using legitimate-looking websites and domain names to lure victims isn't unique to airline ticket fraud. Other types of fraud can be carried out using look-alike web properties. Identifying

cybersquatting domains targeting airlines and digital wallet providers in LAC can help uncover possible vehicles for fraud.

Potential Vehicles for Airline Fraud

Using Domains & Subdomains Discovery, we found 4,576 domains that bore the names of some of the top LAC-based airlines, including Avianca, Volaris, Winair, Aeromexico, Western Air, and Copa Airlines.

The complete list of airlines is shown in the table below, along with the search strings we used and the number of possible cybersquatting domains we found.

Company	Search String	Number of Cybersquatting Domains	Company	Search String	Number of Cybersquatting Domains
Avianca	***avianca***	940	LATAM Airlines	***latamairlines***	100
Volaris	***volaris***	659	Cubana de Aviacion	***cubana*** + ***air***	96
Winair	***winair***	618	Air Caraibes	***aircaraibes***	87
Aerolineas Argentinas	***aerolineas***	581	Azul	***voeazul***	80
Aeromexico	***aeromexico***	447	Caribbean Airlines	***caribbean*** + ***airlines***	68
Western Air	***westernair***	247	Aruba Air	***aruba*** + ***air***	54
Bahamasair	***bahamas*** + ***air***	219	InterCaribbean Airways	***intercaribbean***	44
Copa Airlines	***copaair***	184	Cayman Airways	***caymanairways***	27
Gol	***voegol***	107	Air Antilles	***airantilles***	18

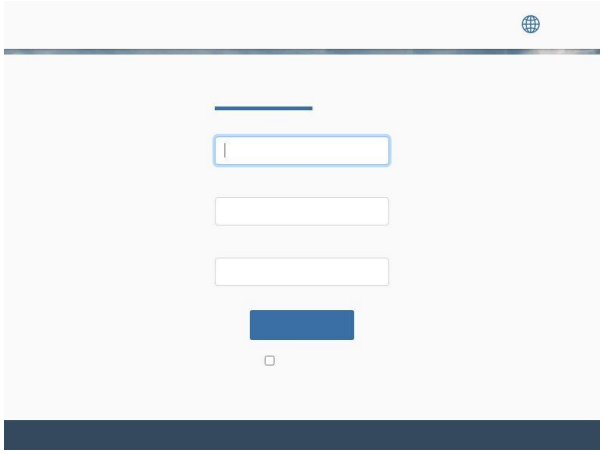
We ran these digital properties on bulk WHOIS and IP lookup tools to perform domain attribution by comparing the results against the IP hosts and WHOIS details of the airline companies' official domains.

Based on the lookup results, less than 1% of the domains could be publicly attributed to the airline companies whose names appeared in the domains. In addition, only 27 of the total

number of cybersquatting domains shared the official domains' IP hosts. On the other hand, only 11 cybersquatting domains could be attributed to the official domains' registrants.

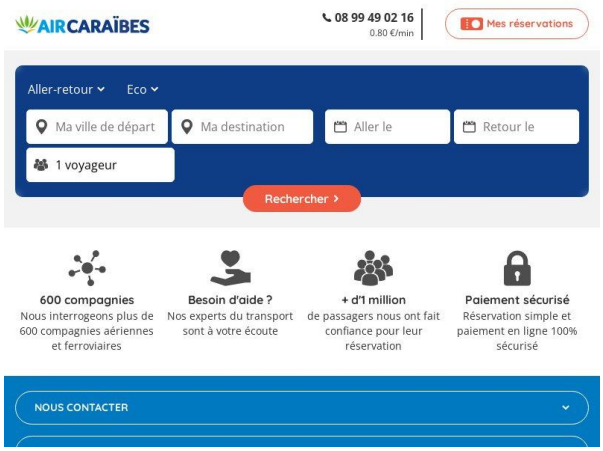
While some of these unattributable domains may be owned and operated by travel agencies and other legitimate businesses, others may not be so innocent. In fact, a few of the domains have already been flagged as malicious, while others like the ones shown below hosted questionable content.

Screenshot of xn--latamairlnes-rgb[.]com



Screenshot of aerolineasclientes[.]com[.]ar

Screenshot of aircaraibes[.]biz



Screenshot of aircaraibesconnect[.]fr

Screenshot of winairsafety[.]com

Screenshot of reservacionesaeromexico[.]com

Note that these login pages looked different from the official login pages of the imitated airline companies.

Potential Vehicles for Fraud Targeting Digital Wallet Users

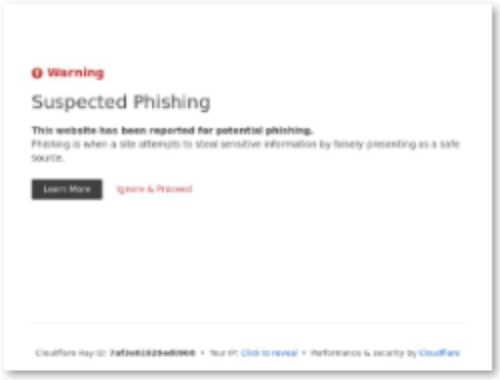
Using the names of some of the most popular digital wallets in LAC as search strings on Domains & Subdomains Discovery, we found 5,047 possible cybersquatting domains. The table below shows the digital wallet providers included in the study, the search strings we used, and the number of cybersquatting properties we found.

Company	Search String	Number of Cybersquatting Domains	Company	Search String	Number of Cybersquatting Domains
Mercado Pago	***mercadopago***	2,003	Inter	***bancointer***	261
Yape	***yape***	1,486	Itau Unibanco - Iti	***iti*** + ***itau***	223
PagBank PagSeguro	***pagseguro***	617	Daviplata	***daviplata***	49
PicPay	***picpay***	408			

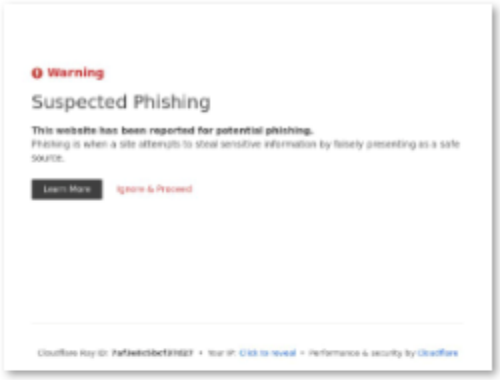
We then retrieved the domains' WHOIS records and IP geolocation details using Bulk WHOIS Lookup and Bulk IP Geolocation Lookup. Based on the results, we found that only a few of the domains could be publicly attributed to the imitated digital wallet providers. Only eight

cybersquatting domains shared the IP hosts of the official domains, while only 12 shared the digital wallet providers' official registrant names.

About 3.4% of the domains imitating the LAC-based digital wallet providers were also found malicious. Some of these domains continued to resolve albeit to warning content.

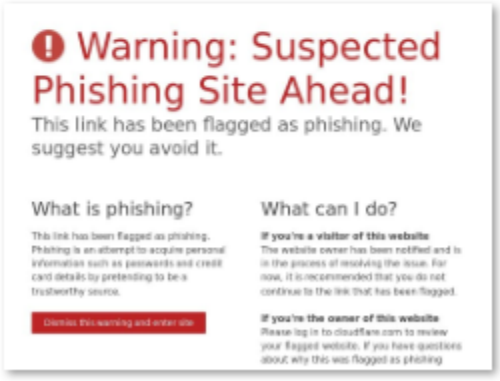


mercadopagocargascom



mercadopagogold

mercadopagonews



mercadopagorun

Extended Threat Discovery

We found a public email address used to register mercadopagorecargar[.]com, one of the malicious domains. Running this on Reverse WHOIS Search, 59 additional domains were discovered. Eight of the connected domains were malicious, including those imitating DirecTV and Spanish bank BBVA.

—

One of the many faces fraud takes is a cybersquatting domain that allows threat actors to bank on the reputation of the imitated company to lure victims in. In this study, we focused on LAC-based airlines and digital wallets and found thousands of potential vehicles for fraud. The same could be said for other sectors and regions, making continuous threat discovery and monitoring critical to fraud and cybercrime prevention.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Artifacts and IoCs

Sample Cybersquatting Domains Targeting LAC-Based Airlines

- 10ansaircaraibes[.]com
- 190nipawinaircadets[.]com
- 190nipawinaircadets[.]org
- 1appsvoeazul[.]com
- 24h-telefonos-info-aerolineas[.]site
- 3avianca[.]com
- aaavianca[.]com
- aaeromexico[.]com
- aavianca[.]com
- abcaerolineas[.]co
- abcaerolineas[.]org
- abqwinair[.]com
- abusosaerolineas[.]com
- abusosaerolineas[.]es
- abusosdeaerolineas[.]com
- abusosdeaerolineas[.]es
- acaribbeanairlines[.]com
- accionistasvolaris[.]com
- aceleradorvolaris[.]com
- aceleradorvolaris[.]com[.]mx
- aclaracionesvolaris[.]com
- acopaair[.]com
- advolaris[.]biz
- advolaris[.]com
- advolaris[.]de
- advolaris[.]eu
- advolaris[.]net
- advolaris[.]org
- aeroavianca[.]com
- aerocaribbeanairlines[.]com
- aerolineaavianca[.]com
- aerolineas[.]aero
- aerolineas[.]app
- aerolineas[.]asia
- aerolineas[.]ca
- aerolineas[.]cc
- aerolineas[.]cl
- aerolineas[.]click
- aerolineas[.]club
- aerolineas[.]cn
- aerolineas[.]co
- aerolineas[.]com
- aerolineas[.]com[.]ar
- aerolineas[.]com[.]au
- aerolineas[.]com[.]br
- aerolineas[.]com[.]cn
- aerolineas[.]com[.]co
- aerolineas[.]com[.]es
- aerolineas[.]com[.]mx
- aerolineas[.]de
- aerolineas[.]es
- aerolineas[.]eu

- aerolineas[.]fr
- aerolineas[.]guru
- aerolineas[.]info
- aerolineas[.]it
- aerolineas[.]lat
- aerolineas[.]mobi
- aerolineas[.]mx
- aerolineas[.]net
- aerolineas[.]net[.]br
- aerolineas[.]news
- aerolineas[.]nu
- aerolineas[.]online
- aerolineas[.]org
- aerolineas[.]pe
- aerolineas[.]plus
- aerolineas[.]press
- aerolineas[.]ru
- aerolineas[.]se
- aerolineas[.]shop
- aerolineas[.]site
- aerolineas[.]tienda
- aerolineas[.]top
- aerolineas[.]travel
- aerolineas[.]uno
- aerolineas[.]us
- aerolineas[.]vacations
- aerolineas[.]vip
- aerolineas[.]website
- aerolineas[.]world
- aerolineas[.]xyz
- aerolineas10[.]com
- aerolineas24[.]es
- aerolineas-24htelefonos-informacion[.]es
- aerolineas-24htelefonos-informacion[.]site
- aerolineasaegentinas[.]com
- aerolineasaereas[.]com
- aerolineasaergentinas[.]com
- aerolineas-aerolineas[.]biz
- aerolineas-aerolineas[.]com
- aerolineas-aerolineas[.]com[.]br
- aerolineas-aerolineas[.]com[.]mx
- aerolineas-aerolineas[.]mx
- aerolineasagentinas[.]com
- aerolineas-aircargo[.]com
- aerolineas-airlines[.]com
- aerolineasalaska[.]com
- aerolineasalbatros[.]com
- aerolineasalmundo[.]com

Sample Cybersquatting Domains Targeting LAC-Based Digital Wallet Providers

- 1clickpagseguro[.]com
- 1cliquepagseguro[.]com
- 1mercadopago[.]com
- 1picpay[.]ru
- 20revendedorpointmercadopago[.]com[.]mx
- 24h-mercadopago[.]com
- 24horas-mercadopago[.]com
- abancointer[.]com
- abstechadsmercadopagobr10[.]com
- accnt-mercadopago[.]com
- account-mercadopago[.]com
- account-mercadopago-pamentos[.]com
- accountpagseguro[.]com
- accounts-secure2mercadopago[.]com
- acessar-mercadopagobr[.]com
- acesseagoraseumercadopago[.]ga
- acessemercadopago[.]ml

- acesseolinkpicpay[.]me
- acesseseumercadopago[.]ga
- acessmercadopago[.]com
- acess-mercadopago[.]xyz
- acesso-clientepagseguro[.]com
- acesso-conta-mercadopago[.]cf
- acessofacilpagseguro[.]com
- acessomercadopago[.]com
- acesso-mercadopago[.]com
- acessomercadopago[.]ga
- acessomercadopago[.]me
- acessomercadopago[.]ml
- acesso-mercadopago[.]ml
- acessomercadopago[.]online
- acessomercadopago[.]tk
- acesso-mercadopago[.]tk
- acesso-mercadopagoo[.]xyz
- acesso-mercadopagoordem[.]online
- acessopagseguro[.]com
- acesso-pagseguro[.]com
- acessopagseguro[.]ml
- acesso-pagseguro[.]ml
- acessopagseguro[.]online
- acesso-pagseguro[.]xyz
- acessopagsegurouol[.]com
- acessopagseguro-uol[.]com
- acesso-picpay[.]xyz
- acessormercadopago[.]com
- acessos-mercadopago[.]cf
- acessos-mercadopago[.]ga
- acessos-mercadopago[.]gq
- acessos-mercadopago[.]ml
- acessos-mercadopago[.]tk
- acreditacion-mercadopago[.]com
- actualizamercadopago[.]com
- adititaunk[.]com
- administrativomercadopago[.]online
- admmercadopago[.]com
- adroitauditing[.]co[.]uk
- adroitauditing[.]com
- ajudabancointer[.]com
- ajudabancointer[.]com[.]br
- ajudamercadopago[.]com[.]br
- ajudamercadopago[.]online
- ajudapicpay[.]com
- ajudapicpay[.]com[.]br
- alerta-mercadopago[.]com
- alertamercadopagoemail[.]com
- alertasmercadopago[.]com
- aletarmercadopago[.]online
- aliadosmercadopago[.]com[.]ar
- allpagseguros[.]com
- alphabancointernational[.]com
- alphabancointernational[.]com[.]ph
- alphabancointernational[.]ph
- amercadopago[.]com
- a-mercadopago[.]com
- analisemercadopago[.]club
- analisemercadopago[.]ml
- analise-mercadopago[.]tk
- aniverpicpay[.]tk
- antendimentomercadopago[.]ml
- anticipoeuronextmercadopago[.]xyz
- apicpay[.]com
- apicpay[.]me
- api-mercadopago[.]ml
- app-acessopagseguro[.]com
- appbancointer[.]cf
- app-bancointer[.]cf
- app-bancointer[.]com
- appbancointerseguro[.]tk
- appbr-mercadopago[.]com
- app-daviplata[.]com
- appicpay[.]cn
- appicpay[.]com
- appicpay[.]net
- appititau[.]com
- appmercadopago[.]cc
- appmercadopago[.]cf
- app-mercadopago[.]cf

- appmercadopago[.]com
- app-mercadopago[.]com
- app-mercadopago[.]ml

Sample Malicious Artifacts Found as of 28 March 2023

- app-mercadopago[.]xyz
- appmercadopagos[.]net
- appmercadopagos[.]net
- app-suportemercadopago-com-br[.]cf
- atendimentomercadopago[.]online
- atendimento-mercadopago[.]online
- automercadopago[.]online
- blog-mercadopagosa[.]com
- carrinho-mercadopago[.]com
- carrinho-mercadopago[.]com
- comprarmaquinadecartaomercadopago[.]com
- confirmacao-onlinemercadopago[.]gq
- contamercadopagoapp[.]tk
- contamercadopagoapp[.]tk
- contas-revalidacao-mercadopago[.]tk
- contas-revalidacao-mercadopago[.]tk
- daviplata[.]store
- daviplata[.]store
- daviplataproteccion[.]com
- daviplataproteccion[.]com
- dispositivos-itauclientes[.]com
- dispositivos-itauclientes[.]com
- itaudispositivo-seguranca[.]com
- itaudispositivo-seguranca[.]com
- iti-itau[.]online
- iti-itau[.]online
- logs-mercadopago[.]gq
- logs-mercadopago[.]ml
- loguinmercadopago[.]com
- maquininhasmercadopago[.]shop
- melhornospicpay[.]com
- melhorpicpaycupom[.]com
- mercadolivre-mp-mercadopago[.]com
- mercadopago[.]asia
- mercadopago[.]br[.]com
- mercadopago[.]gold
- mercadopago[.]gold
- mercadopago[.]help
- mercadopago[.]host
- mercadopago[.]menu
- mercadopago[.]menu
- mercadopago[.]news
- mercadopago[.]news
- mercadopago[.]red
- mercadopago[.]run
- mercadopago[.]run
- mercadopago[.]shop
- mercadopago[.]shop
- mercadopago[.]website
- mercadopagoabuse[.]xyz