中南米・カリブ海地域に特有の潜在的詐欺ドメインを検出

目次

1. 要旨
2. 付録：アーティファクトとIoCの例

要旨

詐欺や不正行為は世界的な問題ですが、一部の地域に特化したものもあるかもしれません。Accertifyは、航空会社やデジタルウォレット業界に関わるものなど、ラテンアメリカ・カリブ海地域（LAC）に特有の傾向をいくつか挙げています。

WhoisXML APIの研究者がこのほど、そうしたLAC特有の傾向を調べて以下を発見しました。

- LACに拠点を置く航空会社を標的にした4,500超のサイバースクワッティングドメイン
- LACに拠点を置く人気デジタルウォレットプロバイダーを標的とした5,000超のサイバースクワッティングドメイン
- 両業界のサイバースクワッティングドメインのうち、なりすまされた企業への帰属が公の情報から確認できたものは1%未満
- 悪意があると判断されたサイバースクワッティングドメインのうち、フィッシングコンテンツをホストしているものが複数
- 60個のドメイン名からなるネットワークに関連付いた1個の悪意あるドメイン名を登録する際に使用された公開の登録者メールアドレス

詐欺の潜在的な媒体を特定

インターポールの説明によれば、航空券詐欺をはたらくサイバー犯罪者は、航空券販売を専門に行なっているかのように見えるウェブサイトを隠れ蓑にします。航空券は盗難またはハッキングされたクレジットカードで購入されたもので、専門業者のように見えるウェブサイトを通じて格安で販売されます。被害者はお得な航空券を見つけたと思うかもしれませんが、最終的には航空券とお金の両方を失うことになるかもしれません。

正規のウェブサイトやドメイン名をかたって被害者を誘うのは、航空券詐欺に限ったことではありません。他の種類の詐欺も見た目が似ているサイトを使用して行われることがあります。

後述の通り、LACの航空会社やデジタルウォレットプロバイダーを標的としたサイバースクワッティングドメインを特定することで、潜在的な詐欺の媒体を発見することができます。

航空会社を装う詐欺の媒体かもしれないドメイン名

まず、当社のDomains & Subdomains Discoveryで検索した結果、Avianca、Volaris、Winair、Aeromexico、Western Air、Copa Airlinesなど、中南米の航空会社の名前を文字列として含んだドメイン名が4,576個見つかりました。

以下はその航空会社のリストです。検索で使った文字列と発見したサイバースクワッティングドメインの数も示しています。

会社名	検索文字列	サイバースクワッティングドメインの数	会社名	検索文字列	サイバースクワッティングドメインの数
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

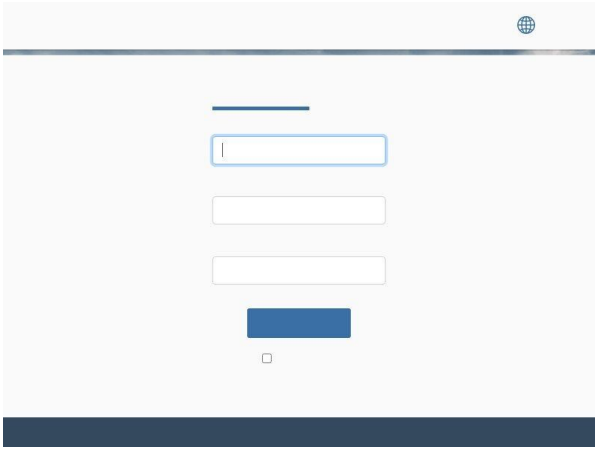
次に、これらのデジタルプロパティをbulk WHOISとIP lookup toolで検索し、航空会社の公式ドメイン名のIPアドレスやWHOISの情報と比較することで、ドメイン名の帰属を検証しました。

その結果、航空会社の社名がドメイン名の中に文字列として含まれ、正規の航空会社への帰属が公開情報から確認できたものは、全体の1%未満にとどまりました。また、サイバースクワッティングドメインのうち、公式ドメイン名と同じIPホストを使っていたドメイン名は27個しかありませんでした。そして、公式ドメイン名の登録者に帰属している可能性のあるサイバースクワッティングドメインは、11件のみでした。

帰属が不明なドメイン名の中には旅行会社などの合法的な企業が所有・運用しているものもありますが、そうでないものもあります。実際、これらのドメイン名の中には、すでに悪意があるというフラグが立っているものもあり、以下に示すような疑わしいコンテンツをホストしているものもあります。

xn--latamairlnes-rgb[.]comの

スクリーンショット

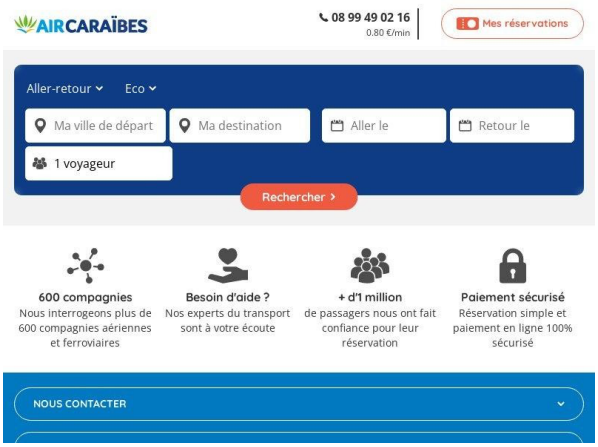


aerolineasclientes[.]com[.]arの

スクリーンショット

aircaraibes[.]bizの

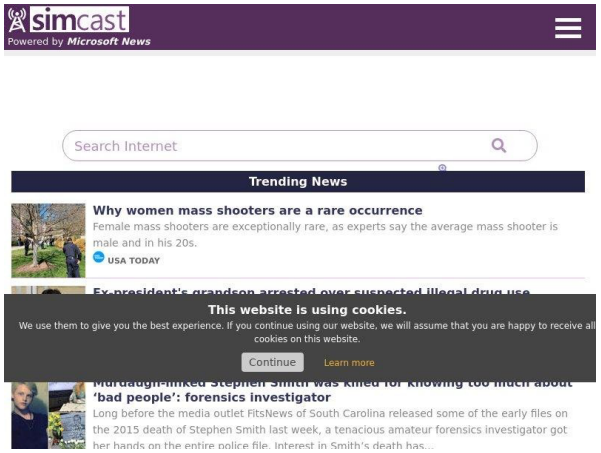
スクリーンショット



aircaraibesconnect[.]frの

スクリーンショット

winairsafety[.]comのスクリーンショット



reservacionesaeromexico[.]comのスクリーンショット

これらのログインページは、航空会社の公式なログインページとは異なるものです。

デジタルウォレットユーザーを狙った詐欺の媒体かもしれないドメイン名

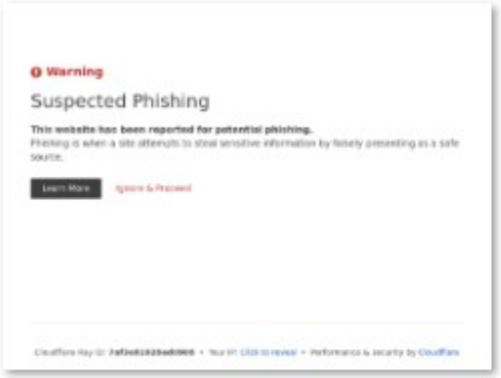
LACで最も人気のあるデジタルウォレットの名前を検索文字列としてDomains & Subdomains Discoveryで調べたところ、サイバースクワッティングの可能性があるドメイン名が5,047個見つかりました。以下の表は、調査の対象となったデジタルウォレットプロバイダー、使用した検索文字列および発見したサイバースクワッティングドメインの数を示しています。

会社名	検索文字列	サイバースクワッティングドメインの数	会社名	検索文字列	サイバースクワッティングドメインの数
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			

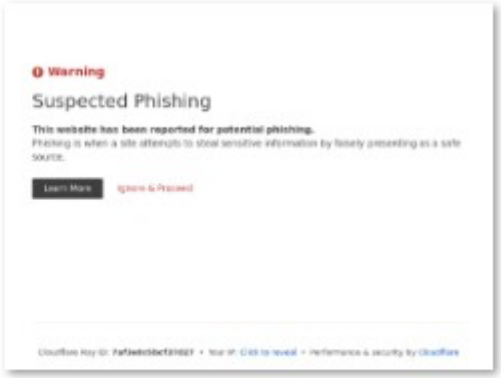
次に、Bulk WHOIS LookupとBulk IP Geolocation Lookupを使用して、ドメイン名のWHOISレコードとIPジオロケーションの情報を取得しました。その結果、デジタルウォレットプロバイダーへの帰属が公開情報から確認できたドメイン名はわずかであることがわかりました。

公式ドメイン名と同じIPアドレスを使っていたサイバースクワッティングドメインは8個、デジタルウォレットプロバイダーの正式な登録者名と同じ登録者名だったサイバースクワッティングドメインは12個でした。

また、LACに本拠を置くデジタルウォレットプロバイダーになりすましたドメイン名の約3.4%は、悪意あるドメイン名でした。これらのドメイン名の一部は、警告コンテンツに到達するとはいえ、名前解決し続けていました。



mercadopagocargascom



mercadopagogold

mercadopagonews

mercadopagorun

さらなる脅威を発見

さらに、悪意あるドメイン名「mercadopagorecargar[.]com」の登録に使用された公開のメールアドレスが1個見つかりました。これをReverse WHOIS Searchにかけたところ、59個のドメイン名が新たに検出されました。それら関連ドメイン名のうち8個は悪意あるもので、DirecTVやスペインの銀行であるBBVAを模倣したものなどがありました。

—

詐欺や不正行為が取るさまざまな形態の1つはサイバースクワッティングドメインで、脅威アクターが正規の企業の評判を利用して被害者をおびき寄せる際に使われます。今回の調査では、LACを拠点とする航空会社とデジタルウォレットに焦点を当て、詐欺の媒体になりうる数千のドメイン名を発見しました。他のセクターや地域でも同様で、不正行為の防止には、こうした脅威の継続的な監視・検知が重要です。

同様の調査をご希望のお客様、または本調査のデーター式をご希望のお客様は、[こちら](#)までお気軽にお問い合わせください。

付録：アーティファクトとIoCの例

LACを拠点とする航空会社を標的としたサイバースクワッティングドメインの例

- 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

LACを拠点とするデジタルウォレットプロバイダーを標的としたサイバースクワッティングドメインの例

- 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

2023年3月28日の時点で確認された悪意あるドメイン名の例

- 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