



Site report for www.americanas.com.br

Netcraft Extension

- Home
- Download Now!
- Report a Phish
- Site Report
- Top Reporters
- Incentives for reporters
- Phishiest TLDs
- Phishiest Countries
- Phishiest Hosters
- Phishiest Certificate Authorities
- Phishing Map
- Takedown Map
- Most Popular Websites
- Branded Extensions
- Tell a Friend

Phishing & Fraud

- Phishing Site Feed
- Hosting Phishing Alerts
- SSL CA Phishing Alerts
- Protection for TLDs against Phishing and Malware
- Deceptive Domain Score
- Bank Fraud Detection
- Phishing Site Countermeasures

Extension Support

- FAQ
- Glossary
- Contact Us
- Report a Bug

Tutorials

- Installing the Extension
- Using the Extension
- Getting the Most
- Reporting a Phish

About Netcraft

- Netcraft Home
- About Netcraft
- Website Terms of Use
- Phishing Site Feed
- Security Services
- Contact Us



Lookup another URL: 

Share:

Enter a URL here

Background


Site title	Not Present	Date first seen	December 1999
Site rank	1810	Primary language	English
Description	Not Present		
Keywords	Not Present		
Netcraft Risk Rating	0/10 <div></div>		
<a href="#">[FAQ]</a>			

Network

Site	<a href="https://www.americanas.com.br">https://www.americanas.com.br</a>	Netblock Owner	Akamai Technologies
Domain	<a href="https://www.americanas.com.br">americanas.com.br</a>	Nameserver	ns-513.awsdns-00.net
IP address	2.18.158.62 ( <a href="#">VirusTotal</a> )	DNS admin	awsdns-hostmaster@amazon.com
IPv6 address	2a02:26f0:6e00:196:0:0:0:19fe	Reverse DNS	a2-18-158-62.deploy.static.akamaitechnologies.com
Domain registrar	nic.br	Nameserver organisation	whois.markmonitor.com
Organisation	B2W - COMPANHIA DIGITAL, Brazil	Hosting company	Akamai Technologies
Top Level Domain	Brazil (.com.br)	DNS Security Extensions	unknown
Hosting country	EU		

SSL/TLS

SSLv3/POODLE	This site does not support the SSL version 3 protocol. <div><a href="#">More information about SSL version 3 and the POODLE vulnerability.</a></div>		
Heartbleed	The site offered the Heartbeat TLS extension prior to the Heartbleed disclosure, but is using a new certificate and no longer offers Heartbeat. <div><div>This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. <a href="#">More information about Heartbleed detection.</a></div></div>		
Assurance	Organisation validation		
Organisation	B2W COMPANHIA DIGITAL	Common name	b2wdigital.com
State	Rio de Janeiro	Country	BR
Organisational unit	Tecnologia	Subject Alternative Name	b2wdigital.com, www.submarino.com, *.thebestoff.com.br, *.b2w.io,

		www.soubarato.com, *.americanas.com.br, *.soubarato.io, *.soubarato.com.br, *.submarino.com.br, *.b2wafp.net, *.shoptime.com.br, *.ad5track.com, *.b2wdigital.com, *.afiliados.com.br, *.b2wads.com, *.atomgtw.com, www.b2wmarketplace.com.br, *.submarino.io, *.shoptime.io, *.americanas.io, www.americanas.com, *.directlog.com.br, *.ame.plus, amedigital.com, b2wmarketplace.com.br, *.bseller.com.br, www.shoptime.com, www.b2wempresas.com, *.b2wempresas.com.br, *.sephora.com.br, *.amedigital.com	
Validity period	From Nov 5 2018 to Feb 4 2020 (14 months, 4 weeks, 1 day)	Matches hostname	Yes
Server	AkamaiGHost	Public key algorithm	rsaEncryption
Protocol version	TLSv1.2	Public key length	2048
Certificate check	ok	Signature algorithm	sha256WithRSAEncryption
Serial number	0x032685dde5c5a2ae141685650b49918b	Cipher	ECDHE-RSA-AES128-GCM-SHA256
Version number	0x02	Perfect Forward Secrecy	Yes
Next Protocol Negotiation	http/1.1,http/1.0	Supported TLS Extensions	<a href="#">RFC5746</a> renegotiation info, <a href="#">RFC4366</a> server name, <a href="#">RFC4492</a> EC point formats, <a href="#">RFC5077</a> session ticket, <a href="#">RFC4366</a> status request, Next Protocol Negotiation
Issuing organisation	DigiCert Inc	Issuer common name	DigiCert SHA2 Secure Server CA
Issuer unit	Not Present	Issuer location	Not Present
Issuer country	US	Issuer state	Not Present
Certificate Revocation Lists	<a href="http://crl3.digicert.com/ssca-sha2-g6.crl">http://crl3.digicert.com/ssca-sha2-g6.crl</a> <a href="http://crl4.digicert.com/ssca-sha2-g6.crl">http://crl4.digicert.com/ssca-sha2-g6.crl</a>	Certificate Hash	v6jI26aEyAnI/IoU2AYV+o6eQBk
Public Key Hash	1fe060712a5a7c2841f160e477da63a35181d0178abd7bf56edd62d3c3a2d7a9		
OCSP servers	<a href="http://ocsp.digicert.com">http://ocsp.digicert.com</a> - 99.70% uptime in the past 24 hours 		
OCSP stapling response	Certificate valid		
OCSP data generated	Jul 10 09:08:57 2019 GMT	OCSP data expires	Jul 17 08:23:57 2019 GMT
Certificate transparency	Signed Certificate Timestamps (SCTs)		
	Source	Log	Timestamp      Signature Verification
	Certificate	Google Pilot	2018-11-05      Success
	pLkJkLQYWBSHux0izGdwCjw1mAT5G9+443fNDsgN3BA=		14:45:29

Certificate	DigiCert 2	2018-11-05	Success
	h3W/5118+IxDmV+9827/Vo1HVjb/SrVgwbTq/16ggw8=	14:45:29	

### SSL Certificate Chain

### Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of [rules](#). Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see [openspf.org](#).

Warning: It appears that this host does not have an SPF record. Setting up an SPF record helps prevent the delivery of forged emails from your domain.

### DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see [dmarc.org](#).

This host does not have a DMARC record.

### Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.


No known trackers were identified.

### Site Technology

Fetchd on 3rd July 2019

### Content Delivery Network

A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers in the Internet. The goal of a CDN is to serve content to end-users with high availability and high performance.

Technology	Description	Popular sites using this technology
Akamai 	Web Content Delivery service provider	<a href="#">www.olx.ua</a> , <a href="#">www.aliexpress.com</a> , <a href="#">www.fidelity.com</a>