



## Netcraft Extension

- ## Phishing & Fraud

- ## Extension Support


- ## Tutorials

- ## About Netcraft


Share:

Enter a URL here

## Background

Site title	Not Present	Date first seen	April 2013
Site rank		Primary language	Unknown
Description	Not Present		
Keywords	Not Present		
Netcraft	1/10		
Risk Rating			
<a href="#">[FAQ]</a>			

## Network

Site	<a href="https://paudosferros.rn.gov.br">https://paudosferros.rn.gov.br</a>	Netblock Owner	HostDime.com, Inc.
Domain	<a href="https://rn.gov.br">rn.gov.br</a>	Nameserver	ns1.rn.gov.br
IP address	162.221.187.234 ( <a href="#">VirusTotal</a> )	DNS admin	suporte@rn.gov.br
IPv6 address	Not Present	Reverse DNS	server.assesi.com
Domain registrar	nic.br	Nameserver organisation	whois.nic.br
Organisation	Governo do Estado do Rio Grande do Norte, Brazil	Hosting company	HostDime.com
Top Level Domain	Brazil (.gov.br)	DNS Security Extensions	unknown
Hosting country	 <a href="#">US</a>		

## SSL/TLS

## SSLv3/POODLE

This site does not support the SSL version 3 protocol.


[More information about SSL version 3 and the POODLE vulnerability.](#)

## Heartbleed

The site offered the Heartbeat TLS extension prior to the Heartbleed disclosure, but is using a new certificate and no longer offers Heartbeat.

This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. [More information about Heartbleed detection.](#)

<b>Assurance</b>	Domain validation		
<b>Organisation</b>	<i>Not Present</i>	<b>Common name</b>	paudosferros.rn.gov.br
<b>State</b>	<i>Not Present</i>	<b>Country</b>	<i>Not Present</i>
<b>Organisational unit</b>	<i>Not Present</i>	<b>Subject Alternative Name</b>	paudosferros.rn.gov.br, www.paudosferros.rn.gov.br
<b>Validity period</b>	From Jul 5 2019 to Oct 3 2019 (2 months, 4 weeks, 1 day)	<b>Matches hostname</b>	Yes
<b>Server</b>	Microsoft-HTTPAPI/2.0	<b>Public key</b>	rsaEncryption

		algorithm	
Protocol version	TLSv1.2	Public key length	2048
Certificate check	ok	Signature algorithm	sha256WithRSAEncryption
Serial number	0x03ccaece78b6a4d62ad9e96b5104c1c408ec	Cipher	ECDHE-RSA-AES256-SHA
Version number	0x02	Perfect Forward Secrecy	Yes
Next Protocol Negotiation	Not Present	Supported TLS Extensions	unknown, <a href="#">RFC5746</a> renegotiation info, <a href="#">RFC4366</a> server name
Issuing organisation	Let's Encrypt	Issuer common name	Let's Encrypt Authority X3
Issuer unit	Not Present	Issuer location	Not Present
Issuer country	US	Issuer state	Not Present
Certificate Revocation Lists	Not Present	Certificate Hash	mOgKg1nVewoptBk8B2nUKrGb1sU
Public Key Hash	28902a8383611ef590c0ceeab1e9beb86980a5ff9ac66b87905807718de5f85e		
OCSP servers	http://ocsp.int-x3.letsencrypt.org - 100% uptime in the past 24 hours 		
OCSP stapling response	No response received		
Certificate transparency	Signed Certificate Timestamps (SCTs)		
	Source	Log	Timestamp
			Signature Verification
	Certificate	Sectigo Mammoth	2019-07-05
		b1N2rDHwMRnYmQCkURX/dxUcEdkCwQApBo2yCJo32RM=	17:08:39
	Certificate	Google Argon 2019	2019-07-05
		Y/Lbzeg7zCzPC3KEJ1drM6SNYXePvXWmOLHhFRL2I0=	17:08:39

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](#).

Qualifier	Mechanism	Argument
+ (Pass)	a	
+ (Pass)	mx	
+ (Pass)	a	server.local
- (Fail)	all	

Modifiers extend the functionality of SPF records. The most common one is the redirect which indicates another host contains the SPF record being searched for.

Modifier	Argument
----------	----------

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](#).

Raw DMARC record:  
v=DMARC1; p=none

Tag	Field	Value
-----	-------	-------

Tag	Field	Value
p=none	Requested handling policy	None: no specific action to be taken regarding delivery of messages.

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 12th July 2019

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
PHP 	PHP is supported and/or running	<a href="http://www.wilderssecurity.com">www.wilderssecurity.com</a> , <a href="http://www.leparisien.fr">www.leparisien.fr</a> , <a href="http://www.mediafire.com">www.mediafire.com</a>
SSL 	A cryptographic protocol providing communication security over the Internet	<a href="http://www.google.com">www.google.com</a> , <a href="http://www.coinbase.com">www.coinbase.com</a> , <a href="http://kayakoreport.hostasaurus.com">kayakoreport.hostasaurus.com</a>


Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Client Pull	No description	<a href="http://www.facebook.com">www.facebook.com</a> , <a href="http://www.sdna.gr">www.sdna.gr</a> , <a href="http://www.asus.com">www.asus.com</a>

Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
X-Frame-Options Same Origin	Do not allow this site to be rendered within an iframe	<a href="http://www.linkedin.com">www.linkedin.com</a> , <a href="http://www.amazon.co.uk">www.amazon.co.uk</a> , <a href="http://www.w3schools.com">www.w3schools.com</a>
X-Content-Type-Options 	Browser MIME type sniffing is disabled	<a href="http://www.googleadservices.com">www.googleadservices.com</a> , <a href="http://www.bitmex.com">www.bitmex.com</a> , <a href="http://dtm.advertising.com">dtm.advertising.com</a>