



# Uma Análise da Utilização de HTTPS no Brasil

**Maurício Fiorenza, Diego Kreutz,  
Thiago Escarrone, Daniel Temp**

# HTTP + TLS



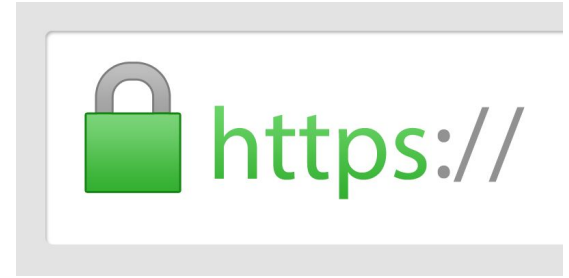
HTTP

Hyper Text  
Transfer Protocol



TLS

Transport Layer  
Security



HTTPS

Hyper Text  
Transfer Protocol  
Secure

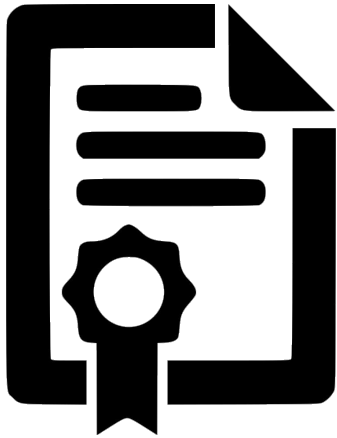
# A falsa sensação de segurança

Cadeado verde  
(ou fechado) é  
sinônimo de  
segurança?



<https://s4a.in/verdeHTTPS>

# Problemas com certificados



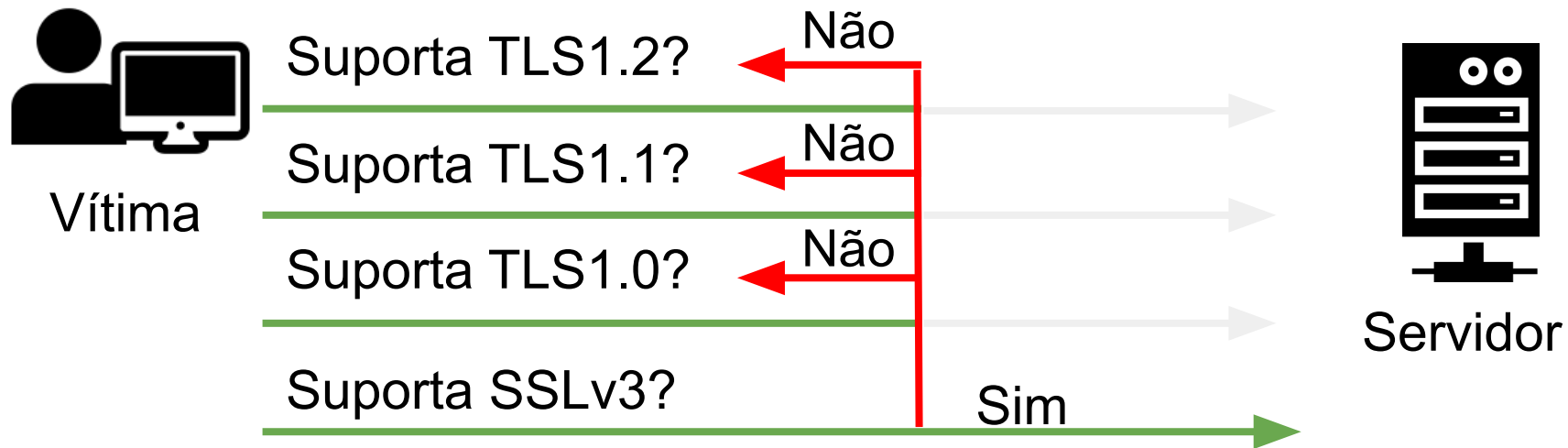
- Certificados auto-assinados
- Hostname não bate com o conteúdo do certificado
- Certificado expirado ou ainda não válido
- Certificados inseguros (chave RSA pequenas ou assinatura com MD5)

<https://s4a.in/badCerts>

# Ataques ao SSL/TLS

Versão	Ataque(s)
SSLv2	DROWN
SSLv3	POODLE, BEAST
TLS 1.0	BEAST
TLS 1.1	POODLE
TLS 1.2	Logjam
TLS 1.3	--

# O ataque POODLE



<https://s4a.in/POODLE>

Atacante (MITM)

# O ataque Logjam (estatísticas)

Protocolo	Vulnerável ao Logjam
HTTPS - Top 1M Domínios	8.4%
HTTPS - Páginas Web	3.4%
SMTP+StartTLS - Endereços IPv4	14.8%
POP3S - Endereços IPv4	8.9%
IMAPS - Endereços IPv4	8.4%

<https://s4a.in/weakDH>

# Diagnósticos de ecossistemas HTTPS

- 2018: 5M IPs analisados na China
  - **66,45% não** fazem uso do HTTPS
  - **33% usam** hash cripto **vulneráveis** (e.g., **MD5**)  
<https://s4a.in/ChinaHTTPS>
- 2018: de 735k sites do Alexa TOP 1M
  - **18,2% usam** a hash cripto **SHA1**  
<https://s4a.in/LookAtTLS>



# **Ecosistema HTTPS no Brasil**

Qual é o estado da saúde do **ecossistema HTTPS no Brasil**?

Quais ferramentas são utilizadas para analisar sites HTTPS?

O TLS 1.3 já é suportado pela maioria dos sites?

Há problemas relacionados aos certificados?

Os algoritmos de assinatura e cifra são os recomendados?

# Roteiro

**Ferramentas de Análise**

**O Ecossistema HTTPS no Brasil**

**Considerações Finais**

# Ferramentas



CipherScan



SSL Checker



# Ferramentas



CipherScan



SSL Checker

Observatory

moz://a



testssl.sh

# Ferramentas



# Ferramentas



CipherScan



SSL Checker



testssl.sh

# Roteiro

Ferramentas de Análise

**O Ecossistema HTTPS no Brasil**

Considerações Finais

# Seleção dos sites



Instituições  
Governamentais

- 20 sites do governo federal
  - presidência, ministérios e agências
- 108 sites do governo estadual
  - site principal + 3 secretarias
- 127 sites do governo municipal
  - capitais + 4 cidades selecionadas pseudo-aleatoriamente



# Seleção dos sites



Instituições  
Financeiras

- 99 instituições filiadas a Febraban
  - apenas sites acessíveis

# Seleção dos sites



E-commerces

- 4458 sites de comércio eletrônico, filiados a Abcomm
  - apenas sites acessíveis

# Seleção dos sites



Base do  
Censys

- 994 sites brasileiros da base do Censys
  - sites acessíveis dos 1000 disponibilizados gratuitamente

# 5806 sites

testssl.sh



20 Governo Federal  
108 Governos Estaduais  
127 Governos Municipais



99 Filiados a Febraban



4458 Fialiados Abcomm



994 IPs da base Censys



## **Análise dos protocolos utilizados**

# 5,1% dos sites **não** suportam HTTPS

Governamentais	16,5%
Financeiros	5%
E-commerces	25,3%
Censys	53,2%

Dos 296 sites  
que **não**  
suportam HTTPS

# 94,9% dos sites suportam HTTPS

Versão	% de sites
<b>SSLv2</b>	<b>2%</b>
<b>SSLv3</b>	<b>5%</b>
TLS 1.0	76%
TLS 1.1	80%
TLS 1.2	97%
TLS 1.3	35%

# 94,90% dos sites suportam HTTPS

Versão	% de sites
SSLv2	2%
SSLv3	5%
<b>TLS 1.0</b>	<b>76%</b>
<b>TLS 1.1</b>	<b>80%</b>
<b>TLS 1.2</b>	<b>97%</b>
TLS 1.3	35%



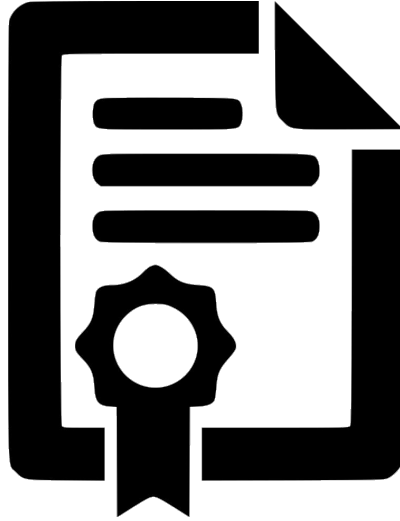
# 94,90% dos sites suportam HTTPS

Versão	% de sites
SSLv2	2%
SSLv3	5%
TLS 1.0	76%
TLS 1.1	80%
TLS 1.2	97%
<b>TLS 1.3</b>	<b>35%</b>

# 94,90% dos sites suportam HTTPS

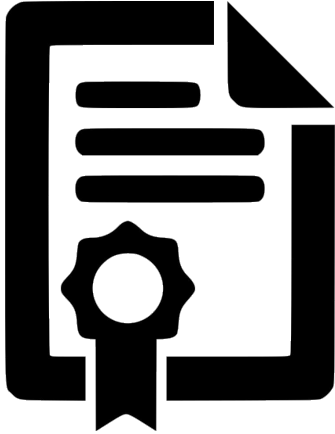
Versão	% de sites
SSLv2	2%
SSLv3	5%
TLS 1.0	76%
TLS 1.1	80%
TLS 1.2	84%
<b>TLS 1.3</b>	<b>35%</b>

**0% dos sites suportam apenas o TLS 1.3**



## **Análise dos Certificados**

# Análise dos certificados



Autoridade Certificadora



Domínio Pertencente



Validade

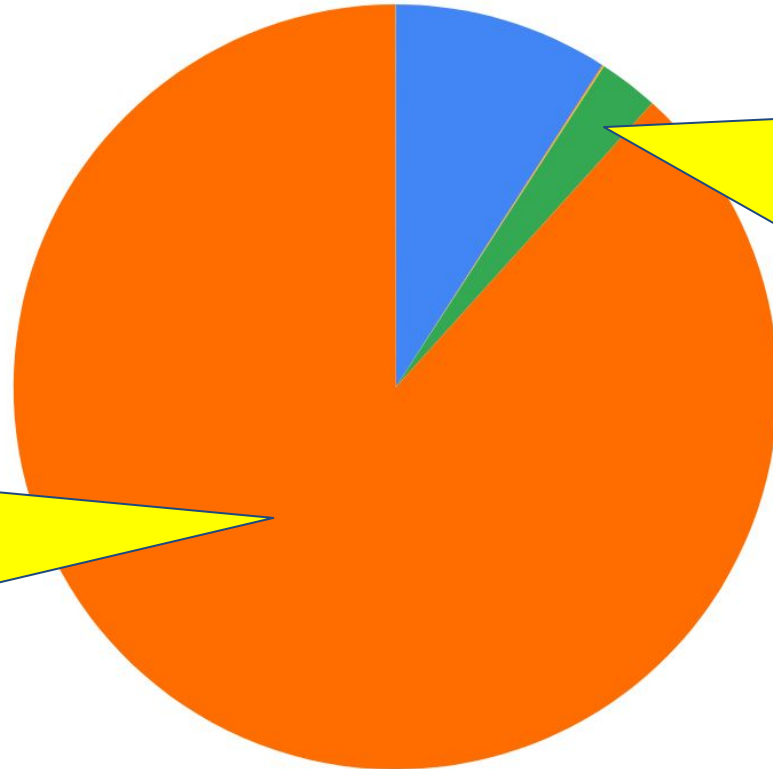
# Análise dos certificados

18% dos sites apresentam problemas de certificado

Certificados auto-assinados	5,5%
Domínio divergente	9,5%
Fora de validade	4,2%

# Algoritmos de assinatura

- ECDSA with SHA256: 502
- ECDSA with SHA384: 2
- RSA with MD5: 3
- RSA with SHA1: 140
- RSA with SHA256: 4882
- RSA with SHA384: 1

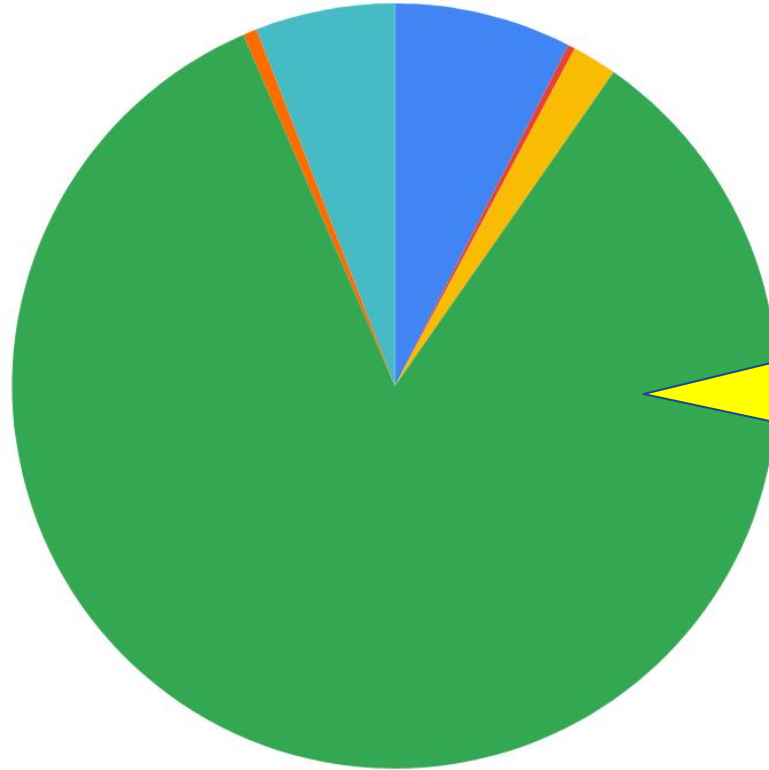


Maioria  
utiliza  
RSA com  
SHA256

Ainda há  
sites que  
utilizam  
MD5 e  
SHA1

# Tamanho da chave

- ECDSA 256: 407
- ECDSA 384: 16
- RSA 1024: 103
- RSA 2048: 4550
- RSA 3072: 32
- RSA 4096: 320



Maioria  
utiliza  
RSA com  
2048 bits



## **Análise dos navegadores e PFS**



# Navegadores e o uso de cifras

<b>Navegador</b>	<b>Cifras recomendadas</b>	<b>Cifras não recomendadas</b>	<b>Sem Conexão</b>
<b>Google Chrome 79</b>	95,60%	4,39%	0,01%
<b>Mozilla Firefox 71</b>	93,32%	6,64%	0,04%
<b>Internet Explorer 11</b>	96,43%	3,57%	0%
<b>Opera 66</b>	95,61%	4,37%	0,02%
<b>Safari 13</b>	94,92%	5,06%	0,02%
<b>Internet Explorer 8</b>	0,90%	71,49%	27,61%

# Navegadores e o uso de cifras

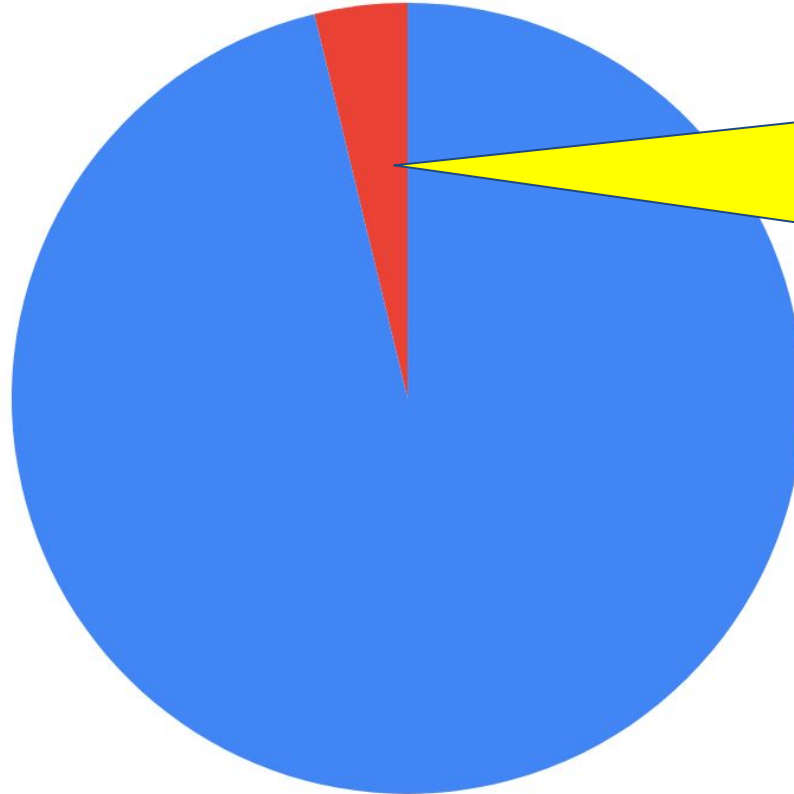
<b>Navegador</b>	<b>Cifras recomendadas</b>	<b>Cifras não recomendadas</b>	<b>Sem Conexão</b>
<b>Google Chrome 79</b>	95,60%	4,39%	0,01%
<b>Mozilla Firefox 71</b>	93,32%	6,64%	0,04%
<b>Internet Explorer 11</b>	96,43%	3,57%	0%
<b>Opera 66</b>	95,61%	4,37%	0,02%
<b>Safari 13</b>	94,92%	5,06%	0,02%
<b>Internet Explorer 8</b>	0,90%	71,49%	27,61%

# Navegadores e o uso de cifras

<b>Navegador</b>	<b>Cifras recomendadas</b>	<b>Cifras não recomendadas</b>	<b>Sem Conexão</b>
<b>Google Chrome 79</b>	95,60%	4,39%	0,01%
<b>Mozilla Firefox 71</b>	93,32%	6,64%	0,04%
<b>Internet Explorer 11</b>	96,43%	3,57%	0%
<b>Opera 66</b>	95,61%	4,37%	0,02%
<b>Safari 13</b>	94,92%	5,06%	0,02%
<b>Internet Explorer 8</b>	0,90%	71,49%	27,61%

# Suporte a Perfect Forward Secrecy (PFS)

- Oferece: 5301
- Não Oferece: 209



apenas  
3,79% dos  
sites não  
oferecem  
PFS

# Roteiro

Ferramentas de Análise

O Ecossistema HTTPS no Brasil

Considerações Finais

# Considerações Finais (resumo)

- **5,10% não** suportam HTTPS
- **100% dos sites** analisados são **vulneráveis**
  - suportam **TLS 1.2 ou inferior**
- **18%** possuem **problemas nos certificados**
- **apenas** 35% suportam o TLS 1.3

# Considerações Finais (demandas)

- Capacitação dos profissionais de TI
  - Conhecimento técnico
  - Diversidade de ferramentas para análise
- Conscientização dos usuários
  - Utilização de navegadores atualizados
  - Observação de alertas de segurança

# Considerações Finais (HTTPS e a LGPD)

- Atender à LGPD requer proteção de dados:
  - armazenados
  - em processamento
  - **em trânsito**



**O HTTPS deve proteger os dados em trânsito!**



# Obrigado!

[mauriciofiorenza@unipampa.edu.br](mailto:mauriciofiorenza@unipampa.edu.br)

[diegokreutz@unipampa.edu.br](mailto:diegokreutz@unipampa.edu.br)

[thiagoescarrone.aluno@unipampa.edu.br](mailto:thiagoescarrone.aluno@unipampa.edu.br)

[danieltemp.aluno@unipampa.edu.br](mailto:danieltemp.aluno@unipampa.edu.br)