unipampa

Universidade Federal do Pampa

HTTPS no Brasil: um estudo empírico

Débora Patrícia Ströher
Orientador: Diego Kreutz

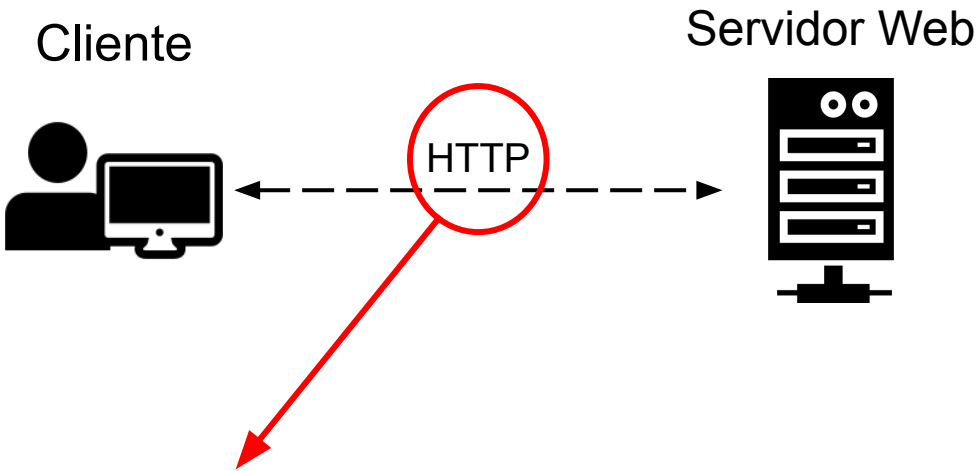
Roteiro

- Introdução
- Ferramentas
- Metodologia
- Resultados
- Considerações Finais

Roteiro

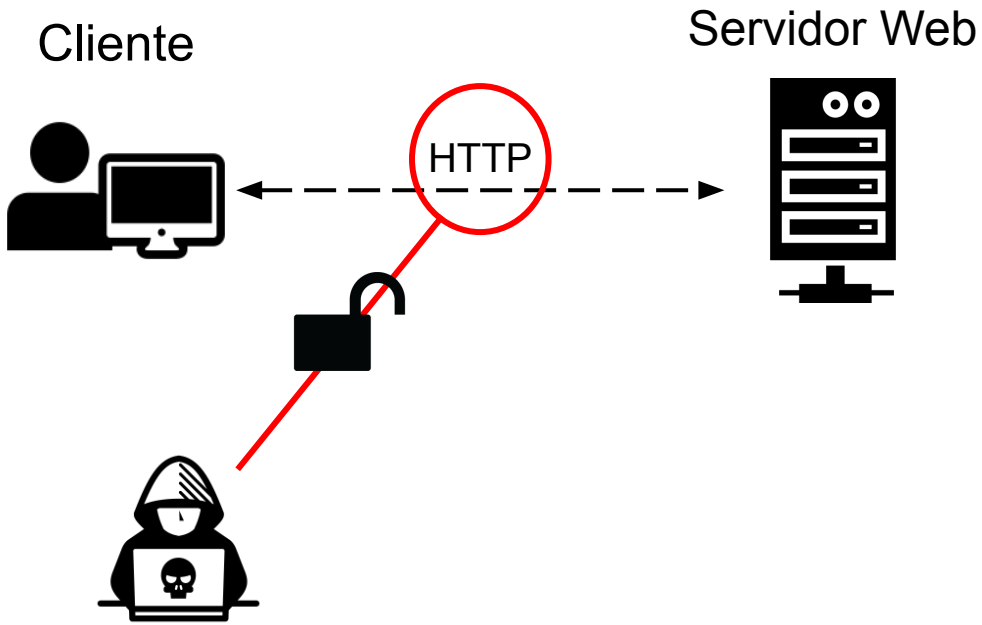
- **Introdução**
- Ferramentas
- Metodologia
- Resultados
- Considerações Finais

HTTP

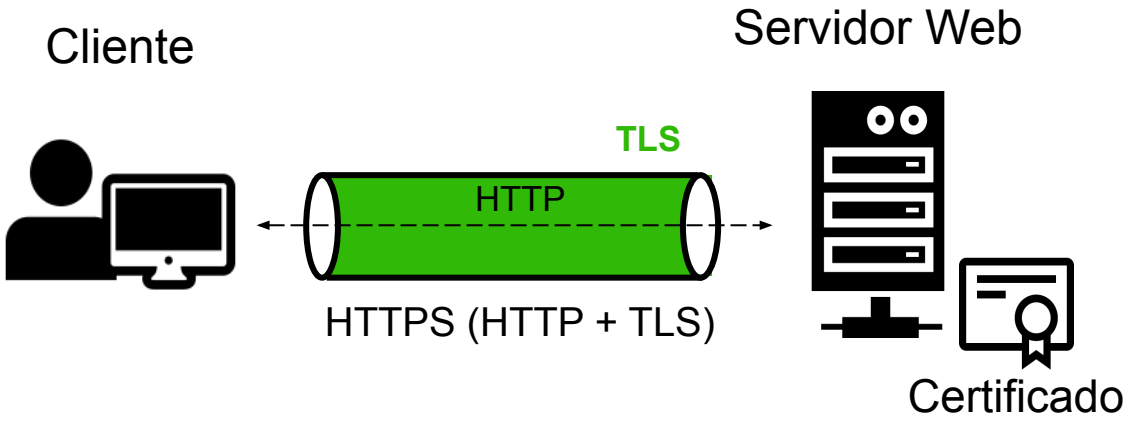


- Protocolo de Transferência de Hipertexto (HTTP)

HTTP



HTTPS



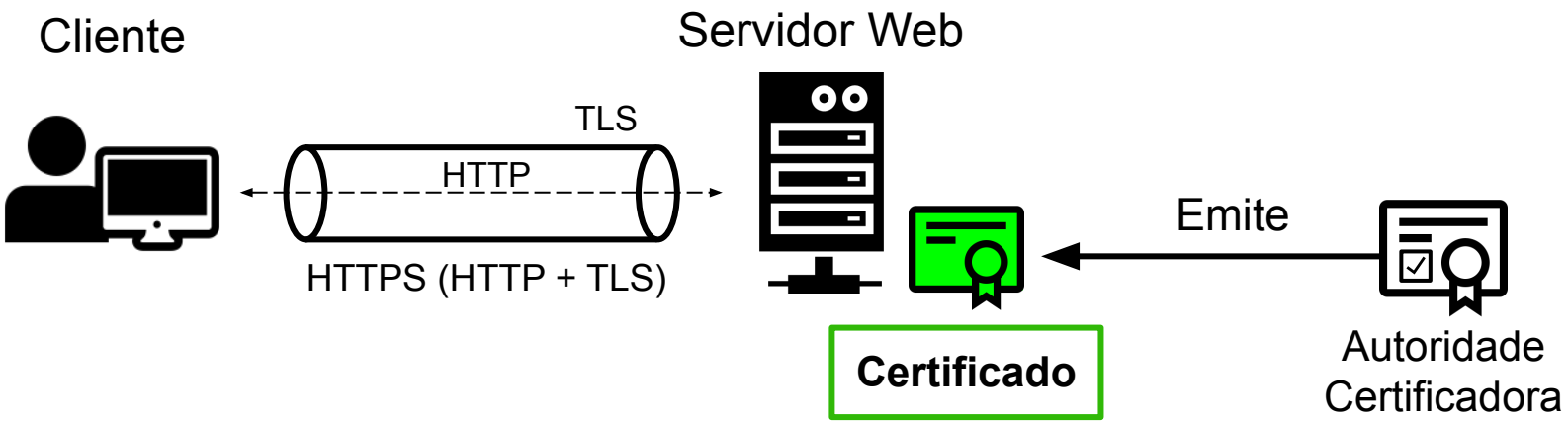
- Protocolo de transferência de hipertexto seguro (HTTPS)

SSL/TLS

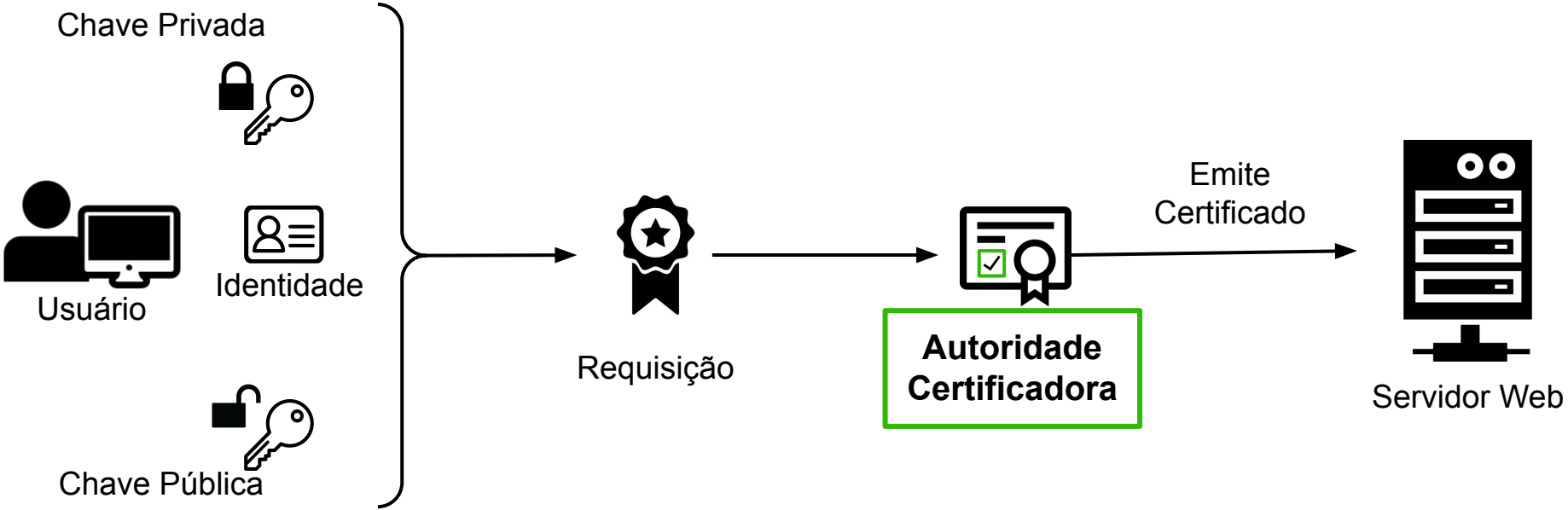
SSL/TLS

- SSL (Secure Sockets Layer) / TLS (Transport Layer Security);
- Principais serviços: Autenticação, encriptação e integridade;

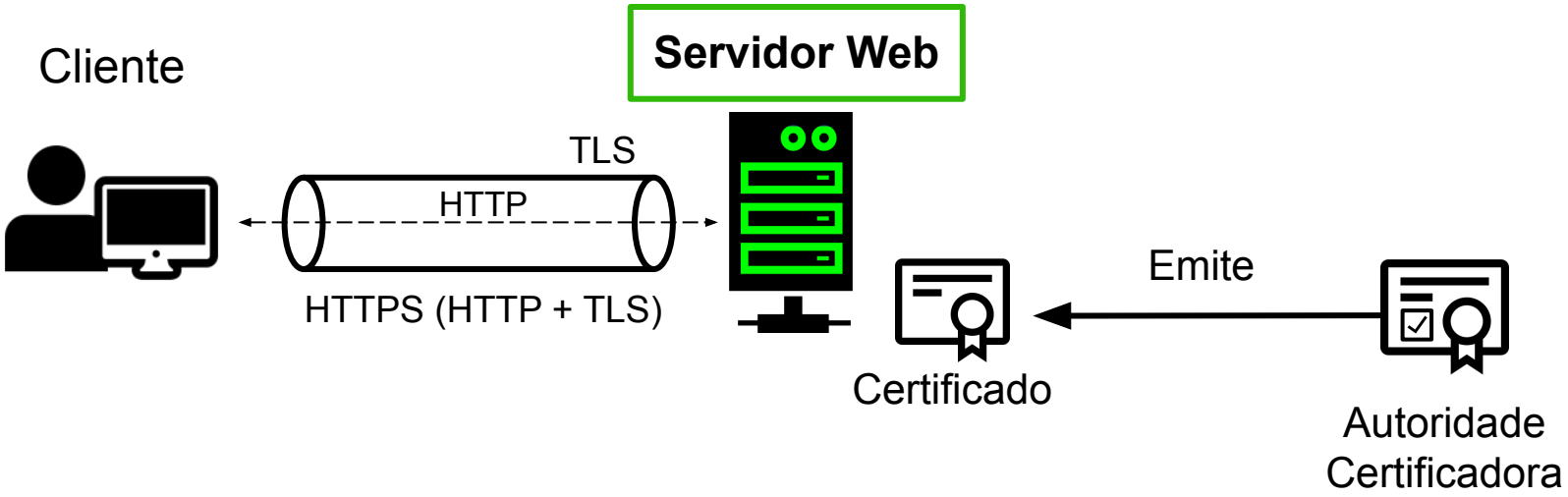
HTTPS


Cliente
Servidor Web
TLS
HTTP
HTTPS (HTTP + TLS)
Emite
Certificado
Autoridade
Certificadora

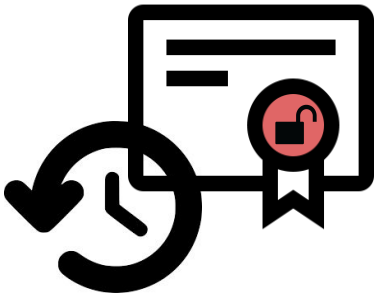
Certificado e Autoridade Certificadora



Certificados nos Servidores Web



Problemas (1/3)



- Certificados não confiáveis dos servidores web
- Certificados autoassinados
- Certificados expirados

Problemas (2/3)

Versão	Ataque(s)	Descrição do Ataque
SSLv2	DROWN	DROWN ataca servidores TLS usando servidor SSLv2, onde existe reúso de certificado e chave.
SSLv3	POODLE, BEAST	POODLE e BEAST exploram vulnerabilidades no modo CBC
TLS 1.0	BEAST	BEAST está relacionado ao Vetor de Inicialização previsível
TLS 1.1	POODLE	POODLE está relacionado ao preenchimento de bloco
TLS 1.2	Logjam	Logjam substitui criptografias fortes por DHE_EXPORT
TLS 1.3	--	--

Problemas (2/3)

Versão	Ataque(s)	Descrição do Ataque
SSLv2	DROWN	DROWN ataca servidores TLS usando servidor SSLv2, onde existe reúso de certificado e chave.
SSLv3	POODLE, BEAST	POODLE e BEAST exploram vulnerabilidades no modo CBC
TLS 1.0	BEAST	BEAST está relacionado ao Vetor de Inicialização previsível
TLS 1.1	POODLE	POODLE está relacionado ao preenchimento de bloco
TLS 1.2	Logjam	Logjam substitui criptografias fortes por DHE_EXPORT
TLS 1.3	--	--

Problemas (2/3)

Versão	Ataque(s)	Descrição do Ataque
SSLv2	DROWN	DROWN ataca servidores TLS usando servidor SSLv2, onde existe reúso de certificado e chave.
SSLv3	BEAST, POODLE	POODLE e BEAST exploram vulnerabilidades no modo CBC
TLS 1.0	BEAST	BEAST está relacionado ao Vetor de Inicialização previsível
TLS 1.1	POODLE	POODLE está relacionado ao preenchimento de bloco
TLS 1.2	Logjam	Logjam substitui criptografias fortes por DHE_EXPORT
TLS 1.3	--	--

Problemas (2/3)

Versão	Ataque(s)	Descrição do Ataque
SSLv2	DROWN	DROWN ataca servidores TLS usando servidor SSLv2, onde existe reúso de certificado e chave.
SSLv3	POODLE, BEAST	POODLE e BEAST exploram vulnerabilidades no modo CBC
TLS 1.0	BEAST	BEAST está relacionado ao Vetor de Inicialização previsível
TLS 1.1	POODLE	POODLE está relacionado ao preenchimento de bloco
TLS 1.2	Logjam	Logjam substitui criptografias fortes por DHE_EXPORT
TLS 1.3	--	--

Problemas (2/3)

Versão	Ataque(s)	Descrição do Ataque
SSLv2	DROWN	DROWN ataca servidores TLS usando servidor SSLv2, onde existe reúso de certificado e chave.
SSLv3	POODLE, BEAST	POODLE e BEAST exploram vulnerabilidades no modo CBC
TLS 1.0	BEAST	BEAST está relacionado ao Vetor de Inicialização previsível
TLS 1.1	POODLE	POODLE está relacionado ao preenchimento de bloco
TLS 1.2	Logjam	Logjam substitui criptografias fortes por DHE_EXPORT
TLS 1.3	--	--

Problemas (2/3)

Versão	Ataque(s)	Descrição do Ataque
SSLv2	DROWN	DROWN ataca servidores TLS usando servidor SSLv2, onde existe reúso de certificado e chave.
SSLv3	POODLE, BEAST	POODLE e BEAST exploram vulnerabilidades no modo CBC
TLS 1.0	BEAST	BEAST está relacionado ao Vetor de Inicialização previsível
TLS 1.1	POODLE	POODLE está relacionado ao preenchimento de bloco
TLS 1.2	Logjam	Logjam substitui criptografias fortes por DHE_EXPORT
TLS 1.3	--	--

Problemas (2/3)

Versão	Ataque(s)	Descrição do Ataque
SSLv2	DROWN	DROWN ataca servidores TLS usando servidor SSLv2, onde existe reúso de certificado e chave.
SSLv3	POODLE, BEAST	POODLE e BEAST exploram vulnerabilidades no modo CBC
TLS 1.0	BEAST	BEAST está relacionado ao Vetor de Inicialização previsível
TLS 1.1	POODLE	POODLE está relacionado ao preenchimento de bloco
TLS 1.2	Logjam	Logjam substitui criptografias fortes por DHE_EXPORT
TLS 1.3	--	--

Problemas (3/3)

- Configurações de cifras nulas e fracas de algoritmos criptográficos

Estudos sobre o Ecossistema HTTPS

Contexto	Quantidade	Problemas
Alexa Top	958,420	16% dos sites implementam HTTPS corretamente
Sites da China	5,002,917	66,45% dos servidores web suportam apenas HTTP 40% dos certificados utilizam algoritmos de resumo criptográficos não recomendados
Sites Brasileiros	5,510	18% implementa incorretamente certificados digitais 80% ainda suportam versões fortemente desaconselhadas do SSL/TLS

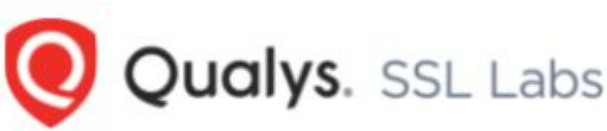
Objetivos

- Levantamento de ferramentas de análise HTTPS
- Ampliar o estudo do ecossistema HTTPS no Brasil
  - Estudo inicial: 5.510 sites
  - Este estudo: 40.406 sites
- Identificar problemas no ecossistema HTTPS

Roteiro

- Introdução
- **Ferramentas**
- Metodologia
- Resultados
- Considerações Finais

Ferramentas (navegador)



Ferramentas (navegador)

Ferramentas (terminal)

CipherScan

OpenSSL
Cryptography and SSL/TLS Toolkit

TestSSLServer

SSLyze

Testing TLS/SSL encryption

Ferramentas (terminal)

CipherScan

OpenSSL
Cryptography and SSL/TLS Toolkit

TestSSLServer

SSLyze

Extensões em navegadores

IndicateTLS

Certificate Pinner

Certainly Something

Extensões em navegadores

IndicateTLS

Certificate Pinner

Certainly Something

Extensões em navegadores

IndicateTLS

Certainly Something

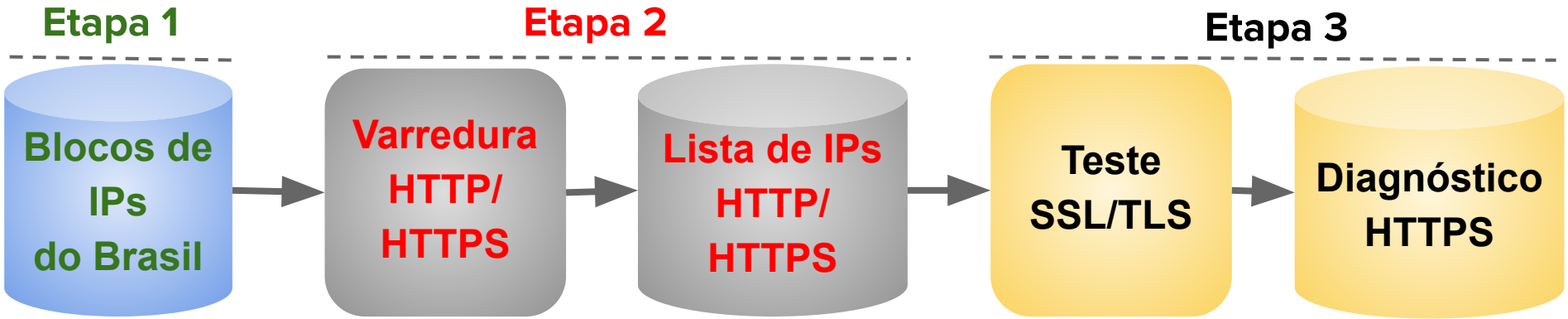
Certificate Pinner

Roteiro

- Introdução
- Ferramentas
- **Metodologia**
- Resultados
- Considerações Finais

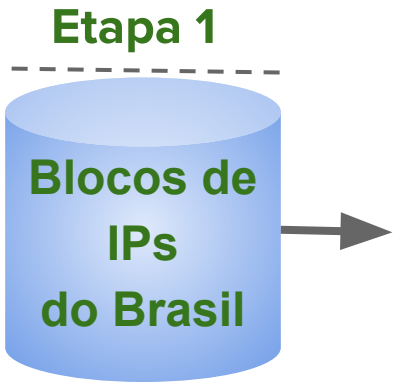
Metodologia

- Processo adotado para a coleta e análise dos dados



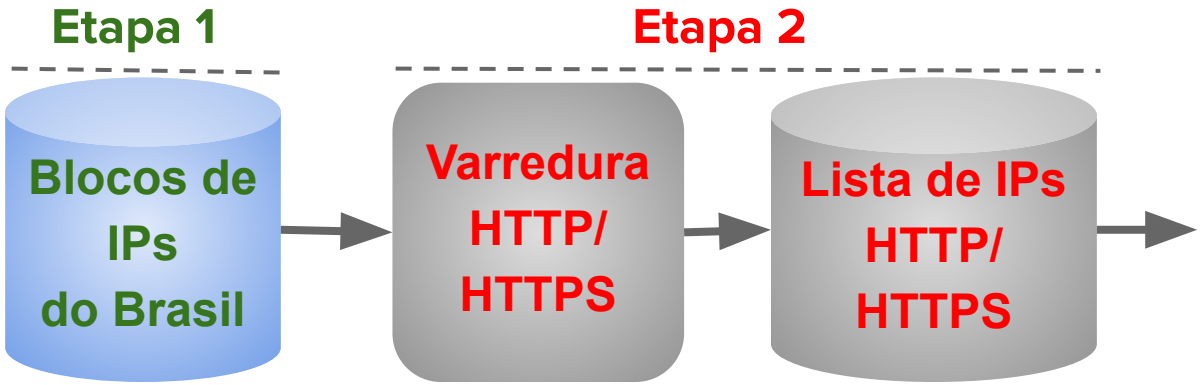
Metodologia

- Processo adotado para a coleta e análise dos dados



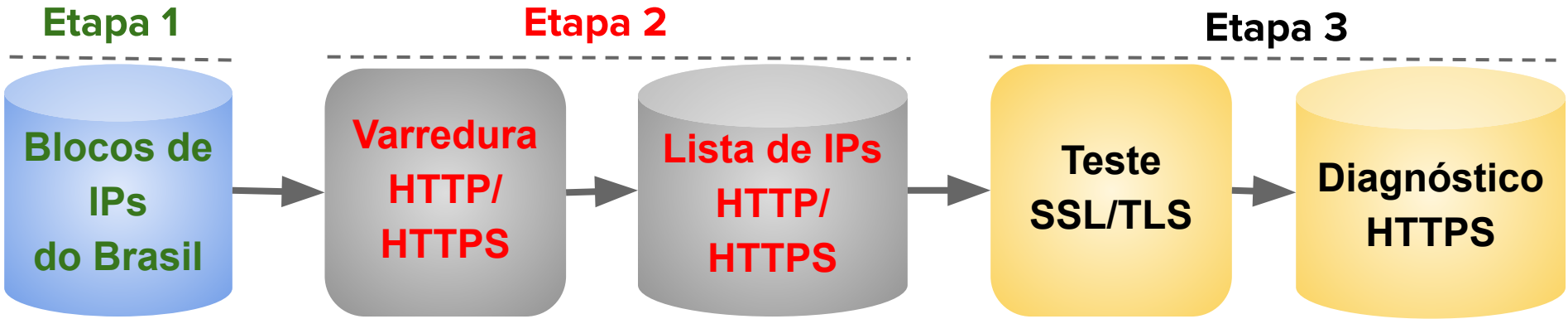
Metodologia

- Processo adotado para a coleta e análise dos dados



Metodologia

- Processo adotado para a coleta e análise dos dados



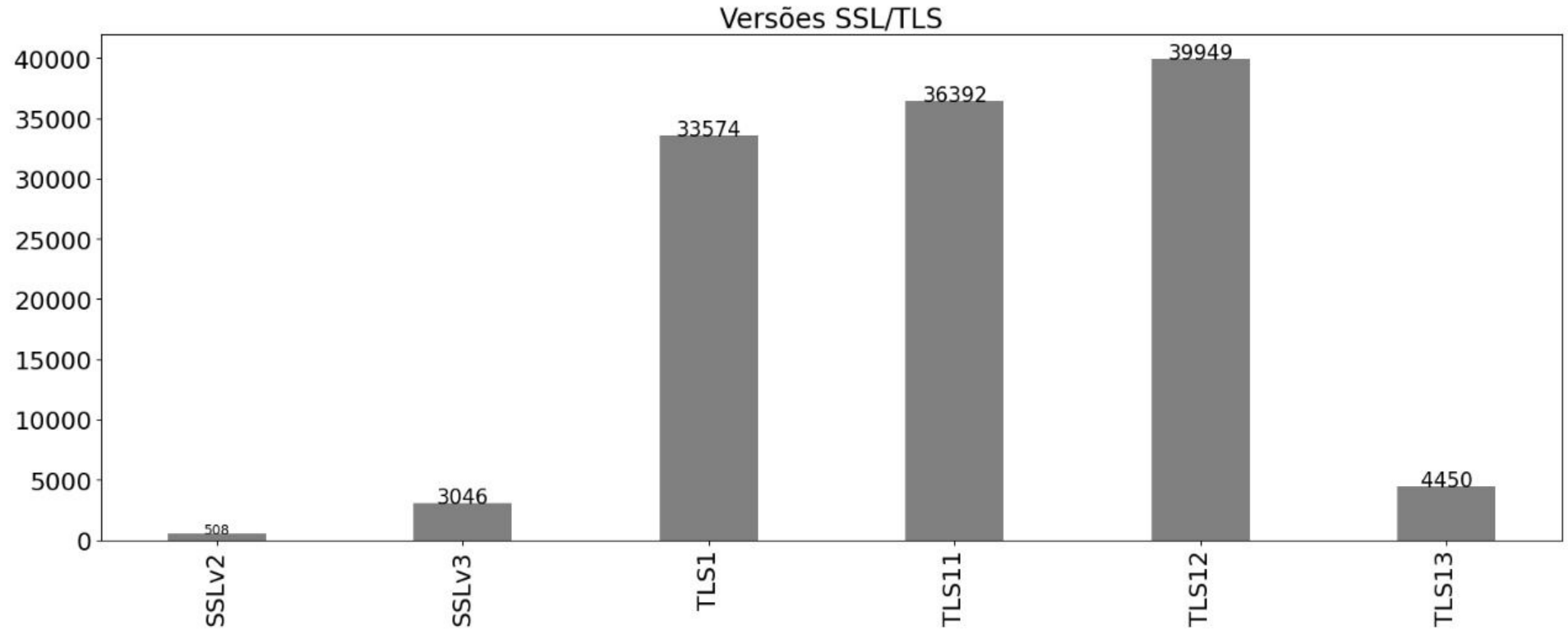
Roteiro

- Introdução
- Ferramentas
- Metodologia
- **Resultados**
- Considerações Finais

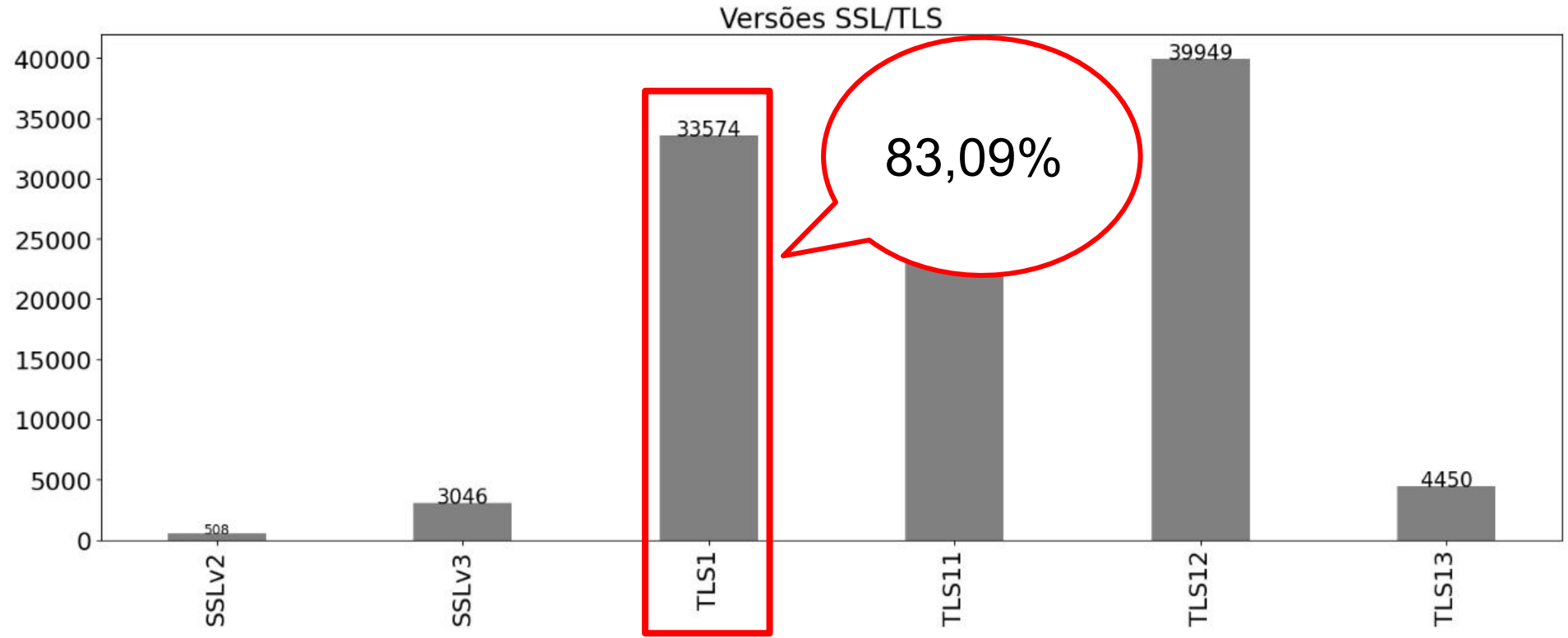
Resultados

- Versões dos Protocolos SSL/TLS
- Emissores dos Certificados
- Cadeia de Confiança
- Validade do Certificado
- Tamanho de Chave
- Ciphers
- PFS
- Algoritmos de Assinatura

Versões dos Protocolos SSL/TLS



Versões dos Protocolos SSL/TLS



Versões dos Protocolos SSL/TLS

		1995	1996	1999	2006	2008	2018
Quantidade de sites	**Ano**	**SSLv2**	**SSLv3**	**TLS 1**	**TLS 1.1**	**TLS 1.2**	**TLS 1.3**
5510	2020	1,82%	5,26%	72,28%	76,00%	92,38%	30,21%
40406	2021	1,25%	7,53%	83,09%	90,06%	98,86%	11,01%

Versões dos Protocolos SSL/TLS

		1995	1996	1999	2006	2008	2018
Quantidade de sites	**Ano**	**SSLv2**	**SSLv3**	**TLS 1**	**TLS 1.1**	**TLS 1.2**	**TLS 1.3**
5510	2020	1,82%	5,26%	72,28%	76,00%	92,38%	30,21%
40406	2021	1,25%	7,53%	83,09%	90,06%	98,86%	11,01%

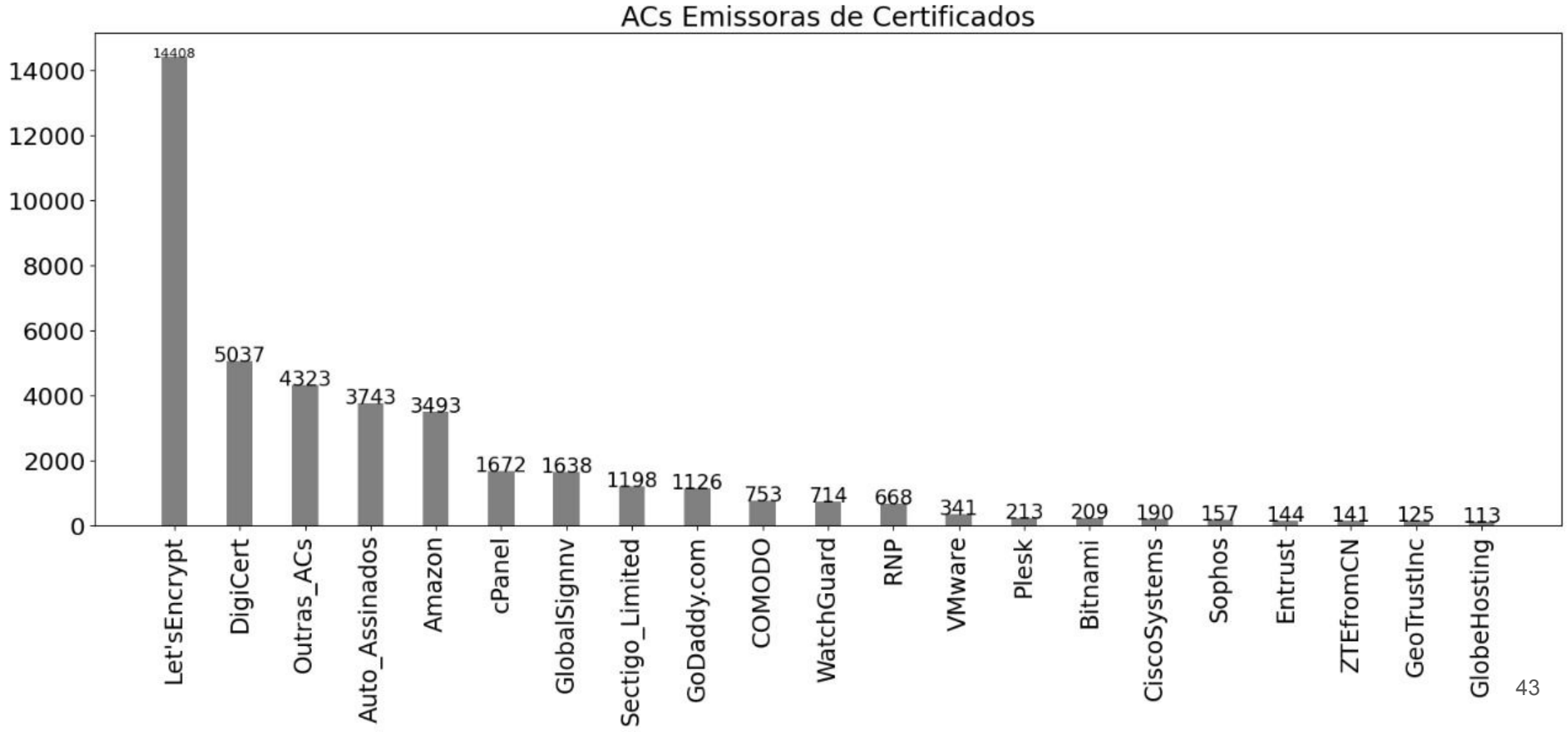
Versões dos Protocolos SSL/TLS

		1995	1996	1999	2006	2008	2018
Quantidade de sites	**Ano**	**SSLv2**	**SSLv3**	**TLS 1**	**TLS 1.1**	**TLS 1.2**	**TLS 1.3**
5510	2020	1,82%	5,26%	72,28%	76,00%	92,38%	30,21%
40406	2021	1,25%	7,53%	83,09%	90,06%	98,86%	11,01%

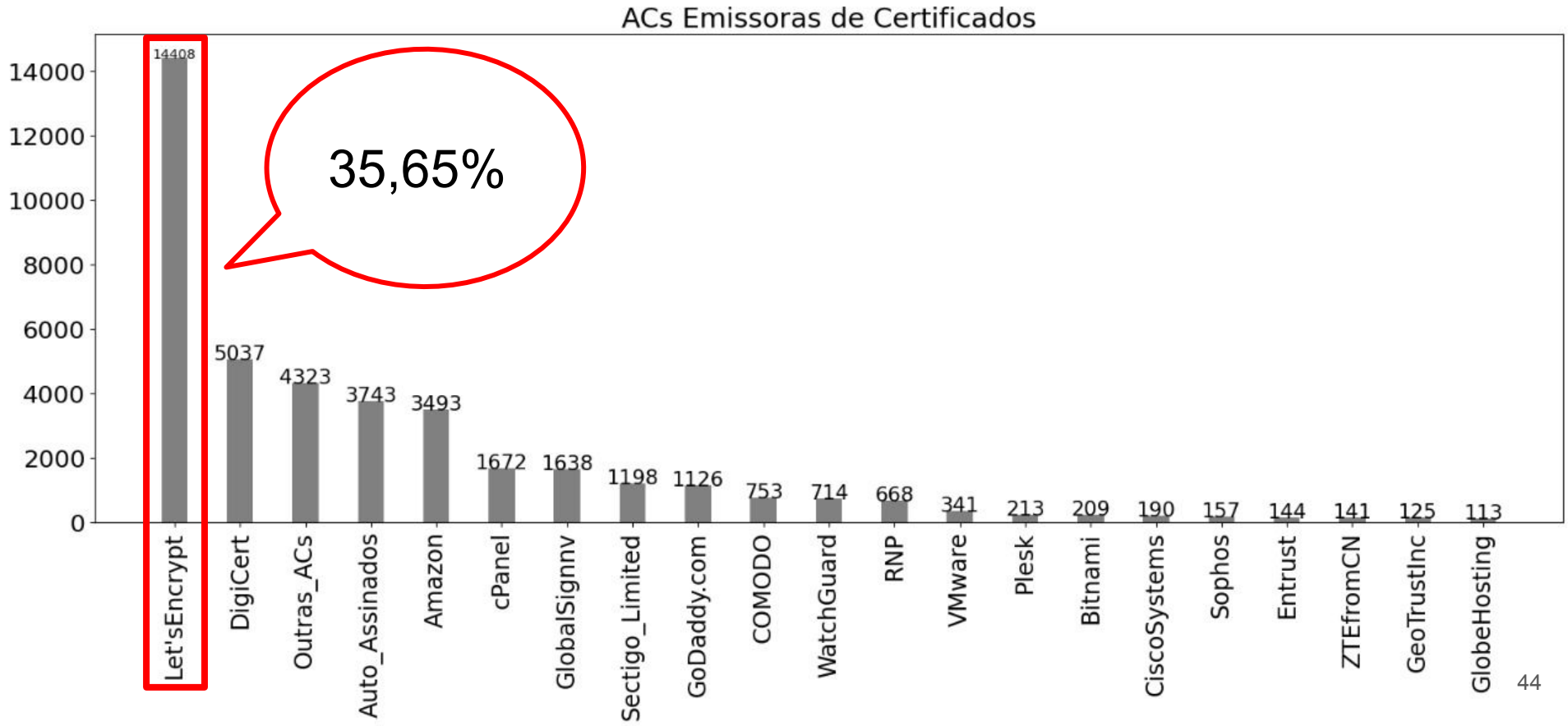
Versões dos Protocolos SSL/TLS

		1995	1996	1999	2006	2008	2018
Quantidade de sites	**Ano**	**SSLv2**	**SSLv3**	**TLS 1**	**TLS 1.1**	**TLS 1.2**	**TLS 1.3**
5510	2020	1,82%	5,26%	72,28%	76,00%	92,38%	30,21%
40406	2021	1,25%	7,53%	83,09%	90,06%	98,86%	11,01%

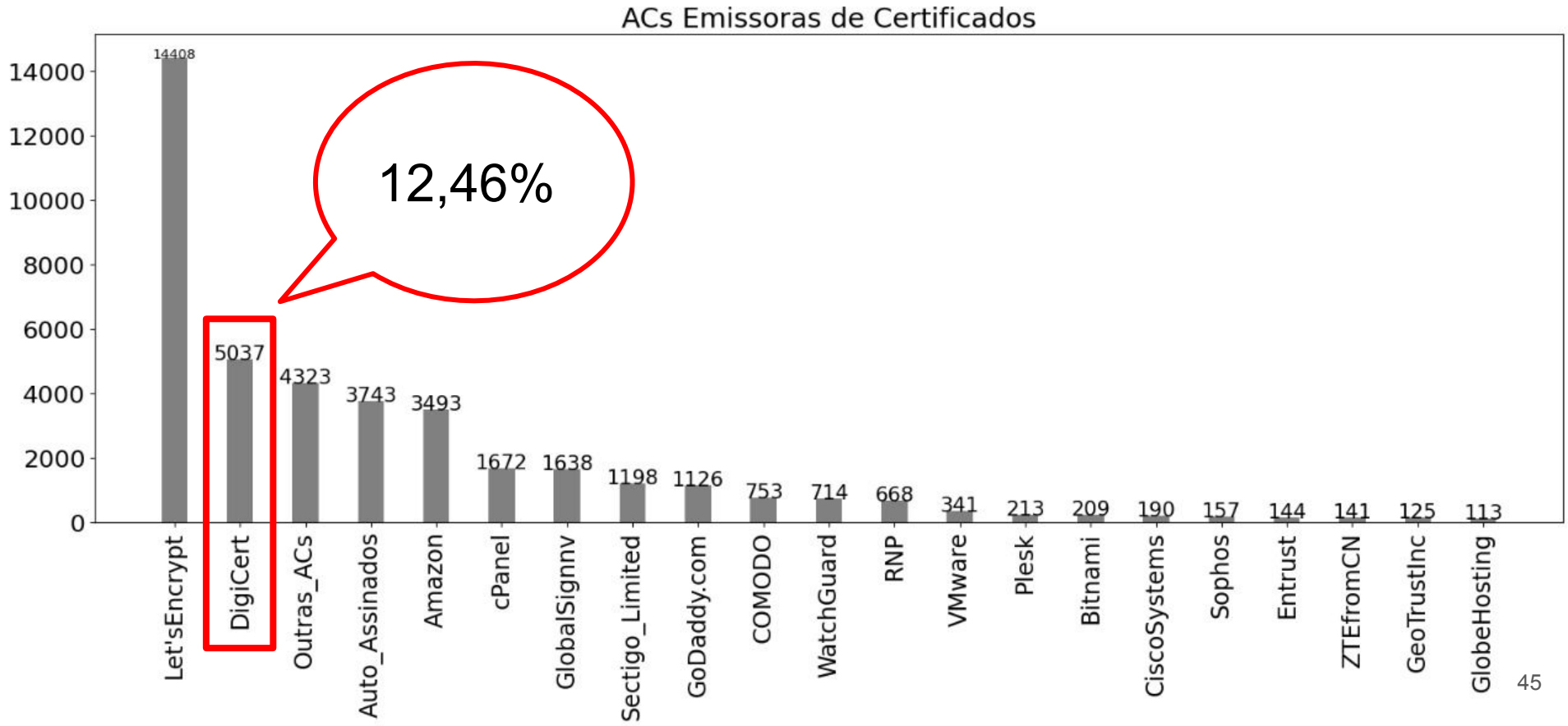
Emissores dos Certificados



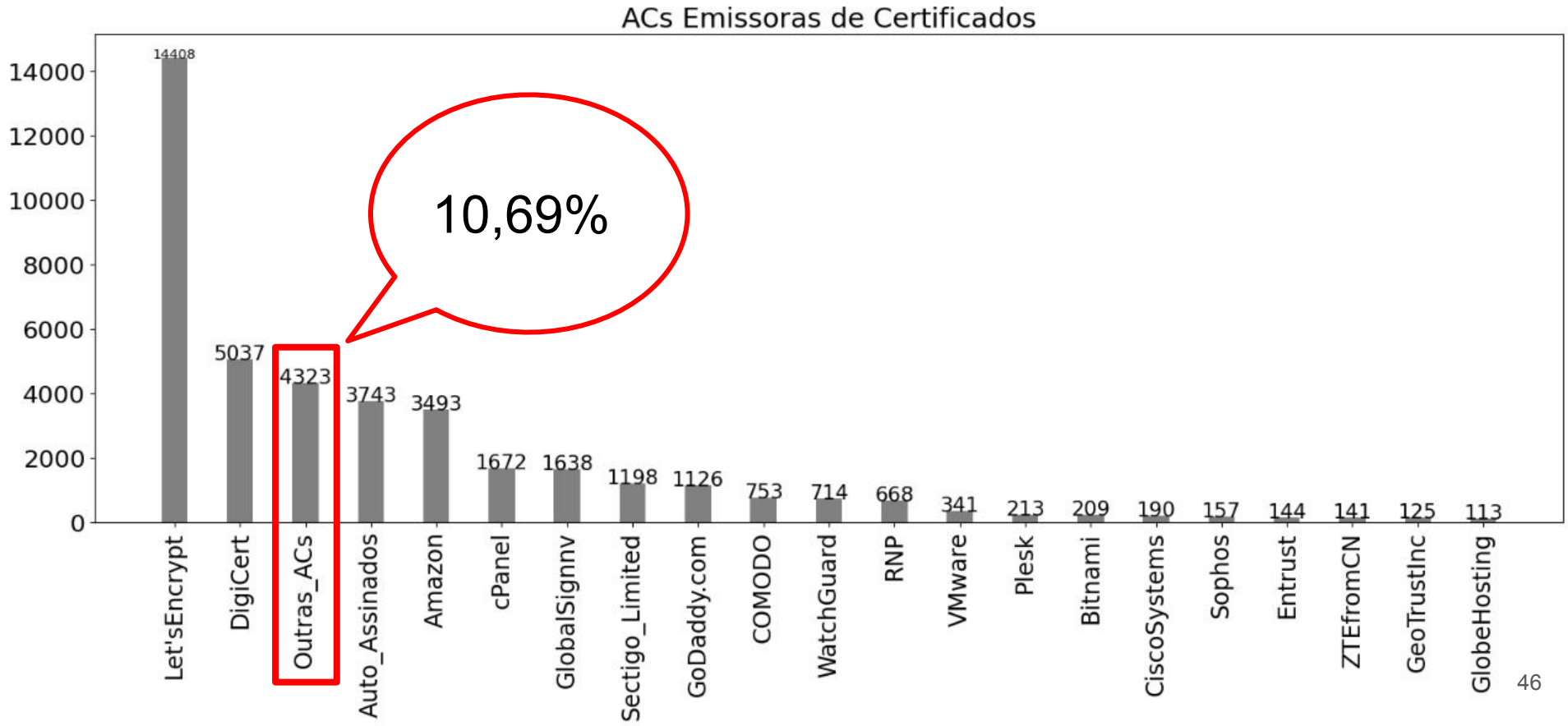
Emissores dos Certificados



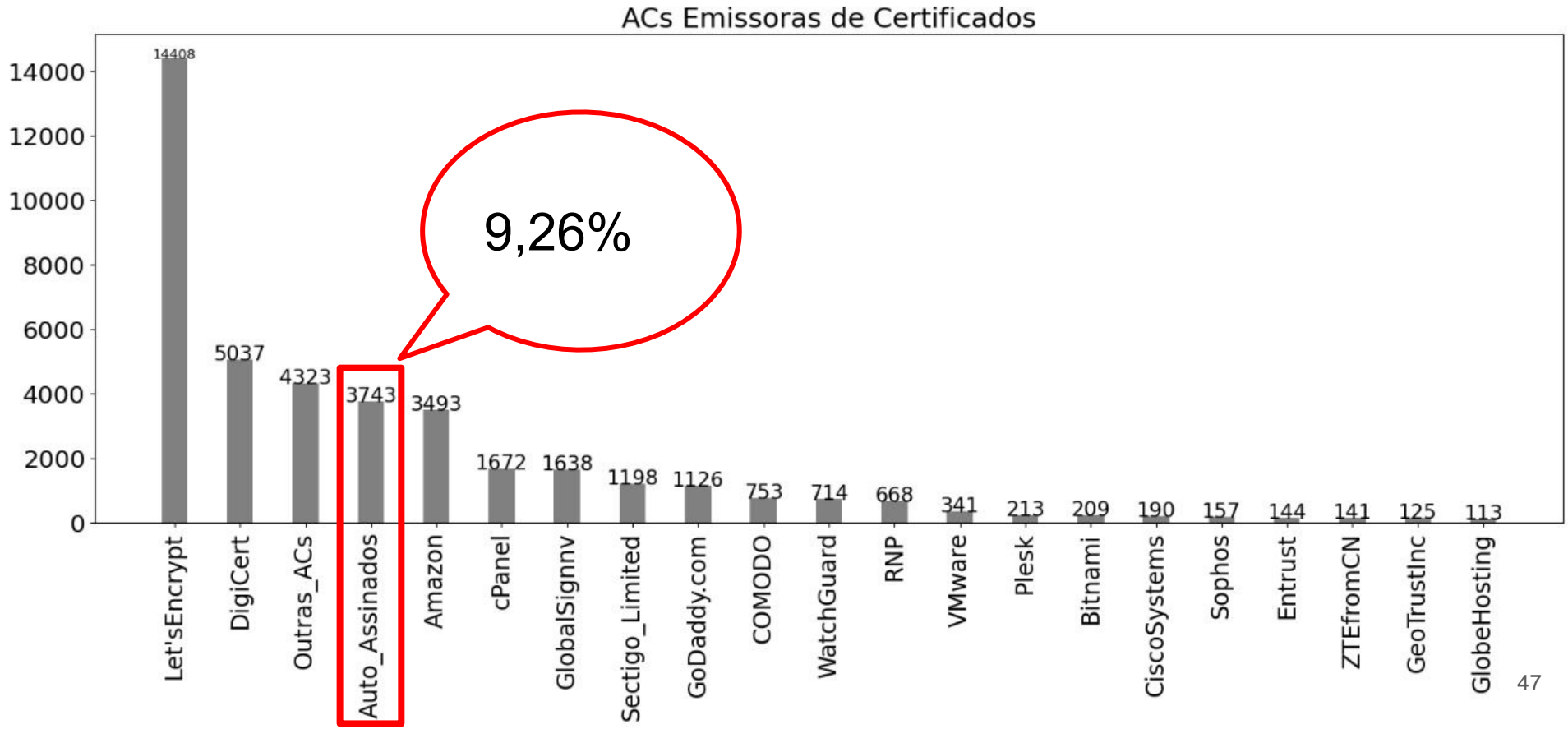
Emissores dos Certificados



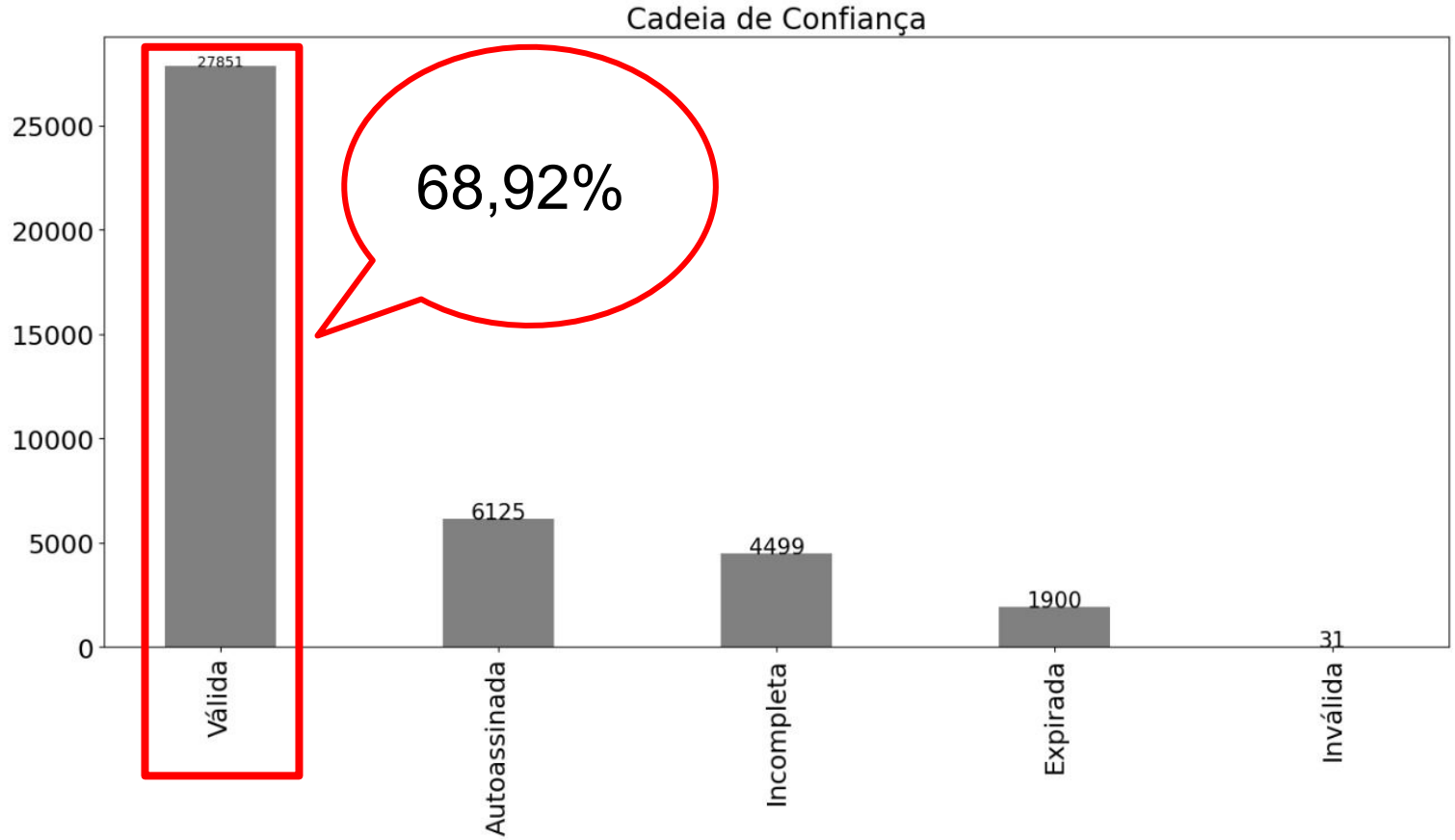
Emissores dos Certificados



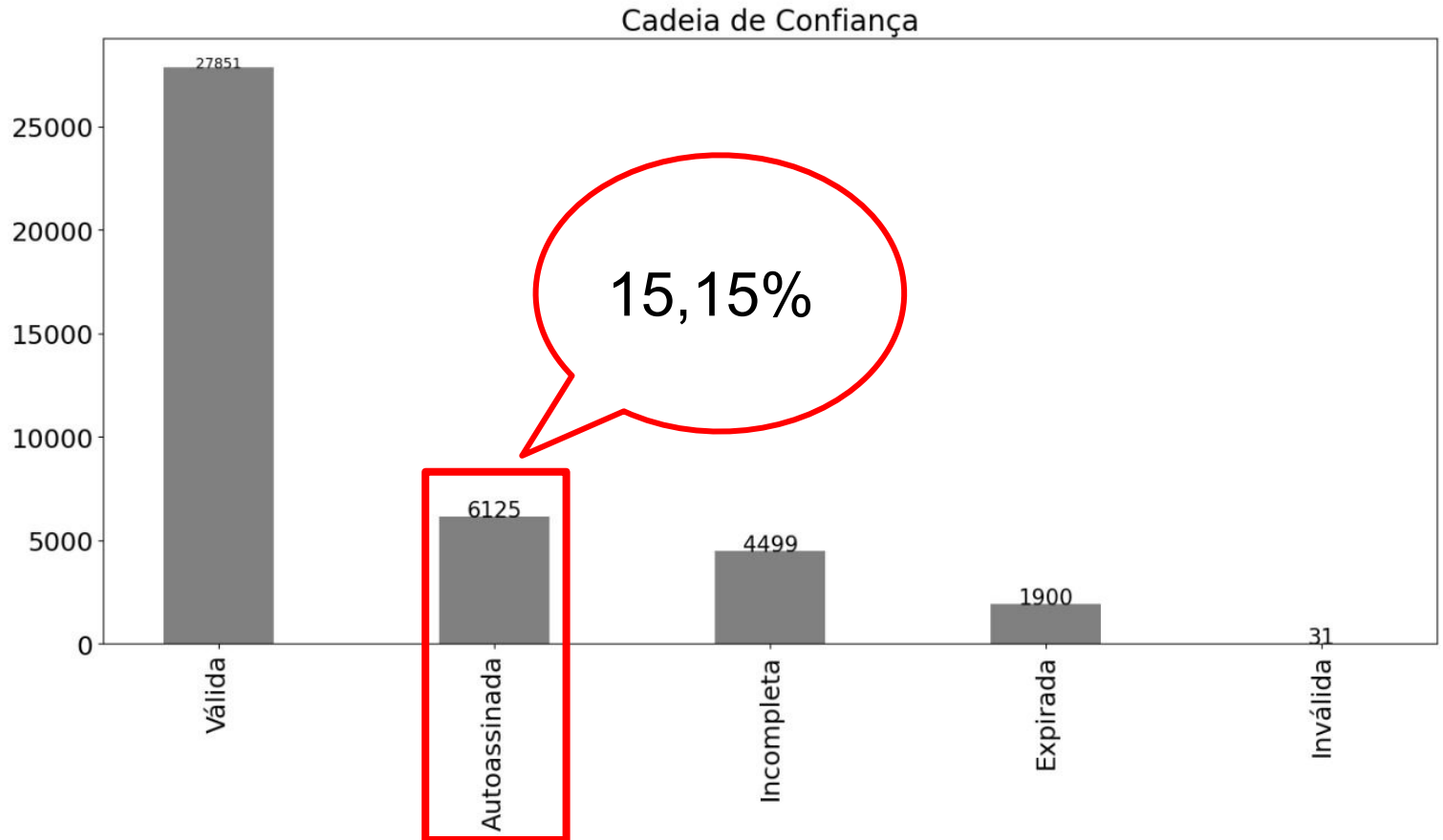
Emissores dos Certificados



Cadeia de Confiança



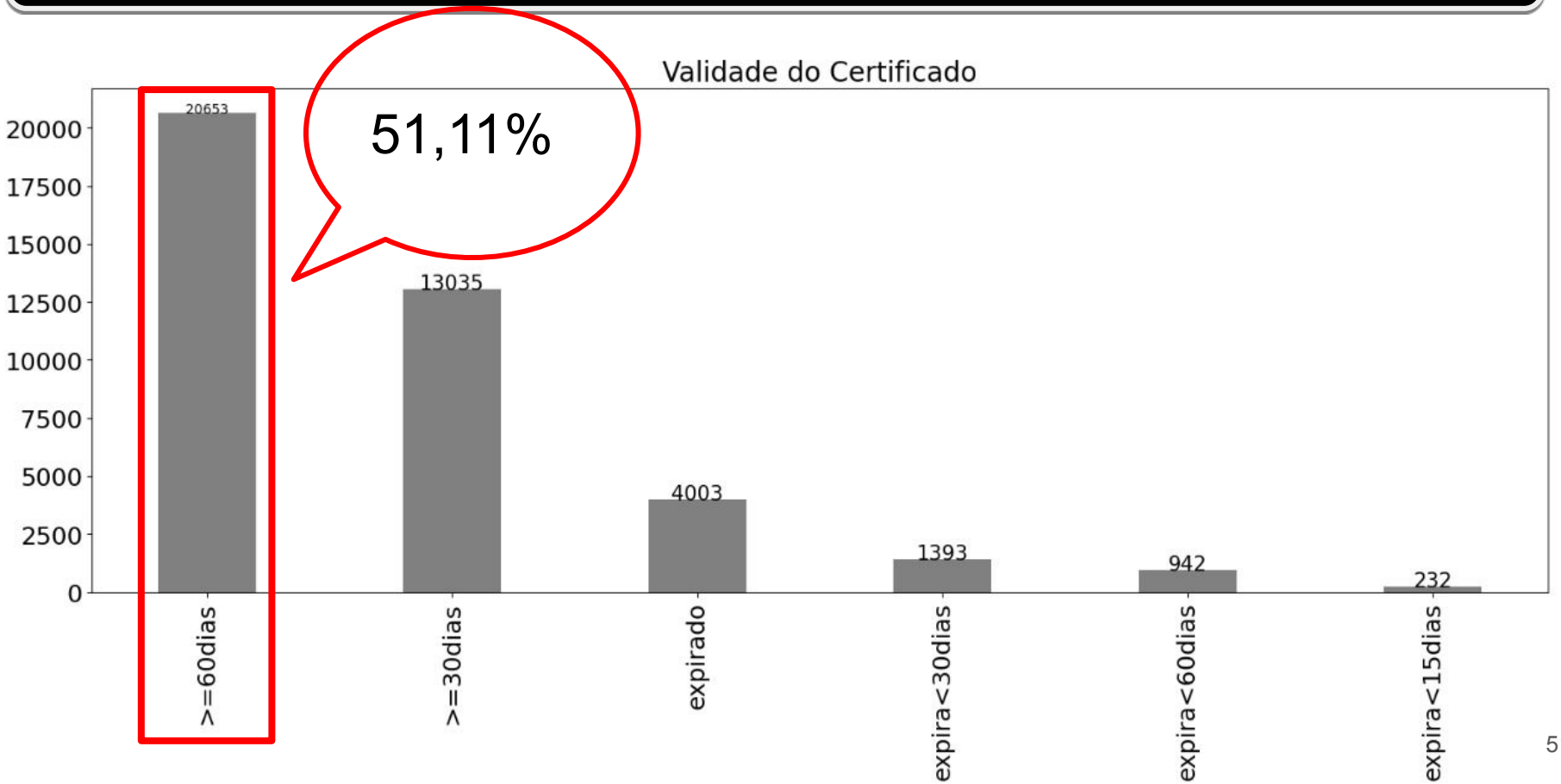
Cadeia de Confiança



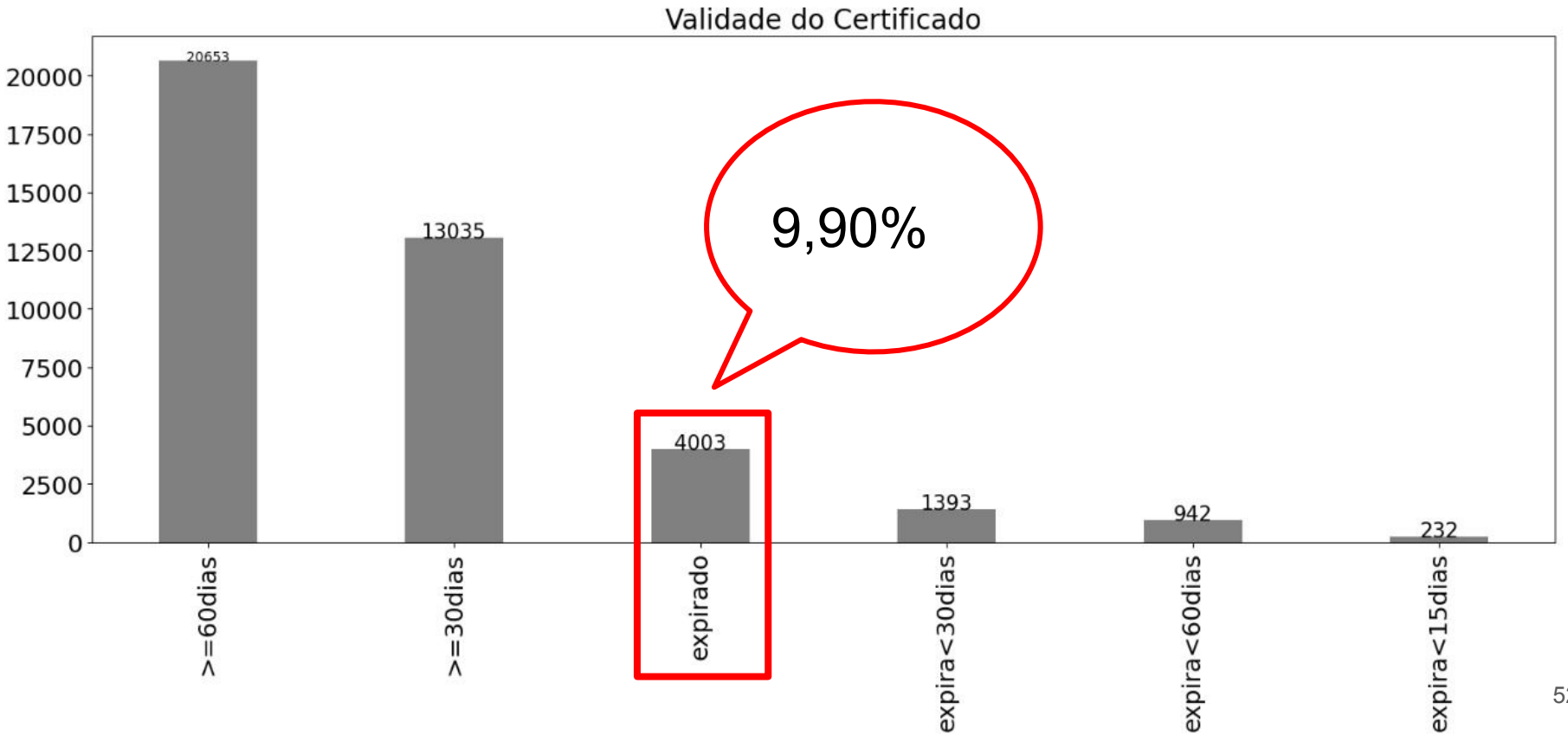
Cadeia de Confiança

Quantidade de sites	Ano	Incompleta	Autoassinada	Expirada
5510	2020	12,83%	5,49%	4,22%
40406	2021	11,13%	15,15%	4,70%

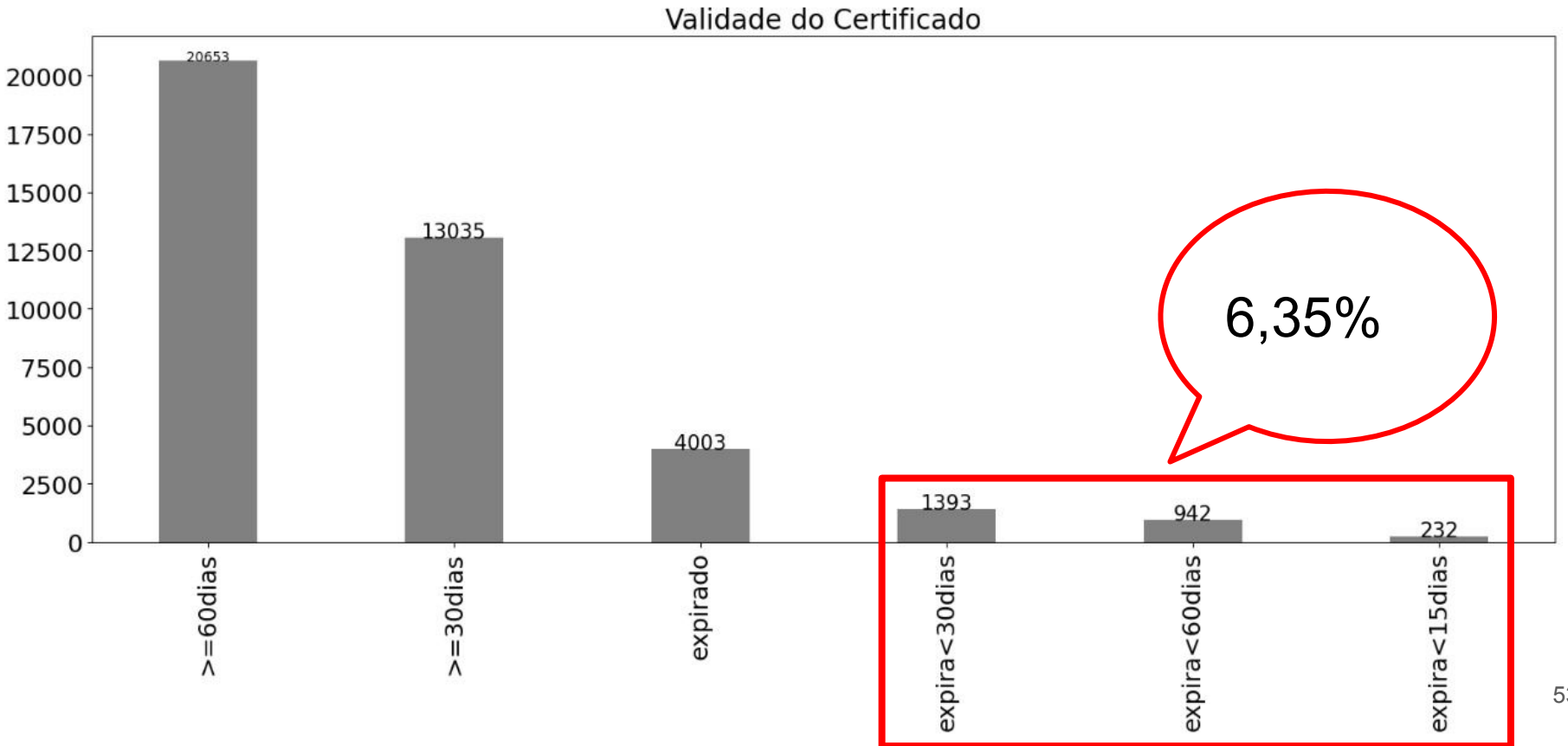
Validade do Certificado



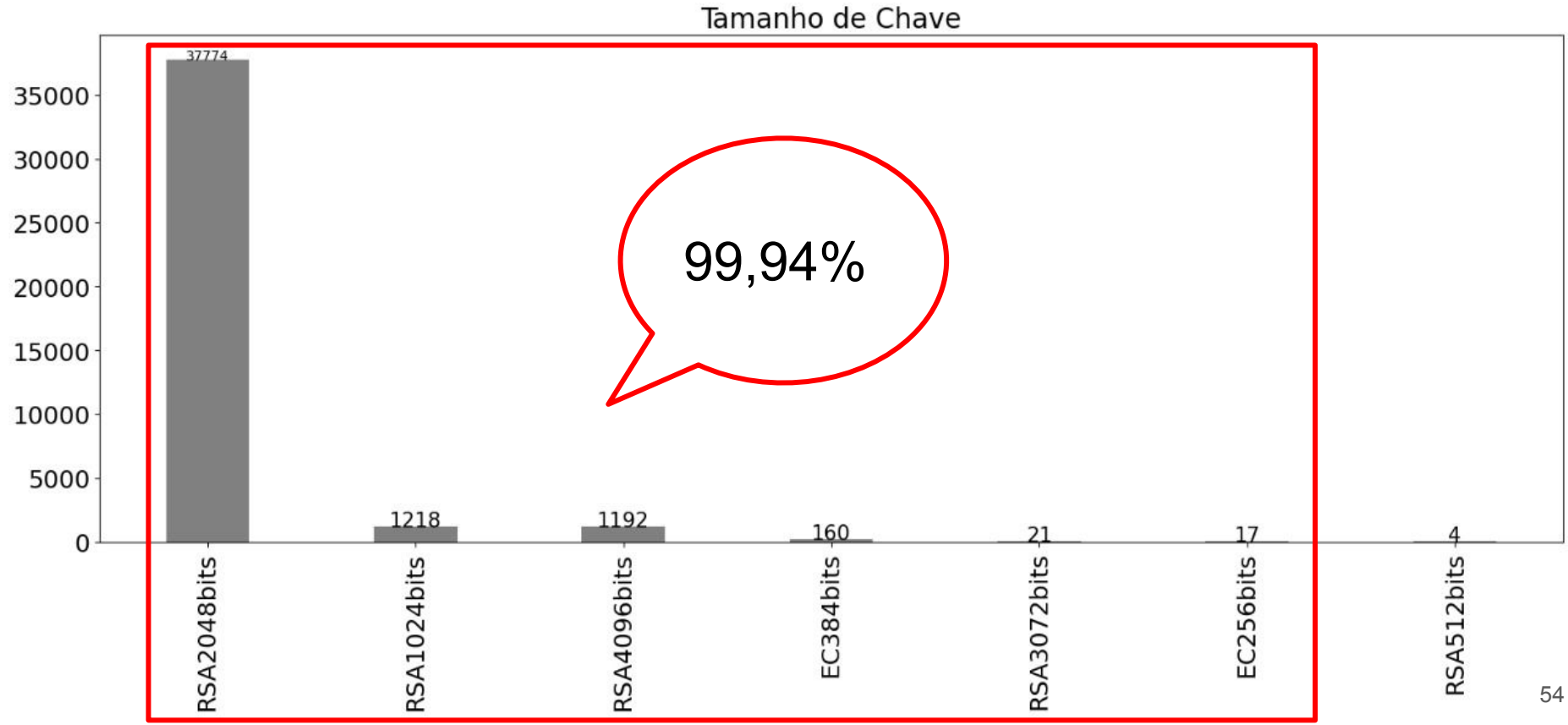
Validade do Certificado



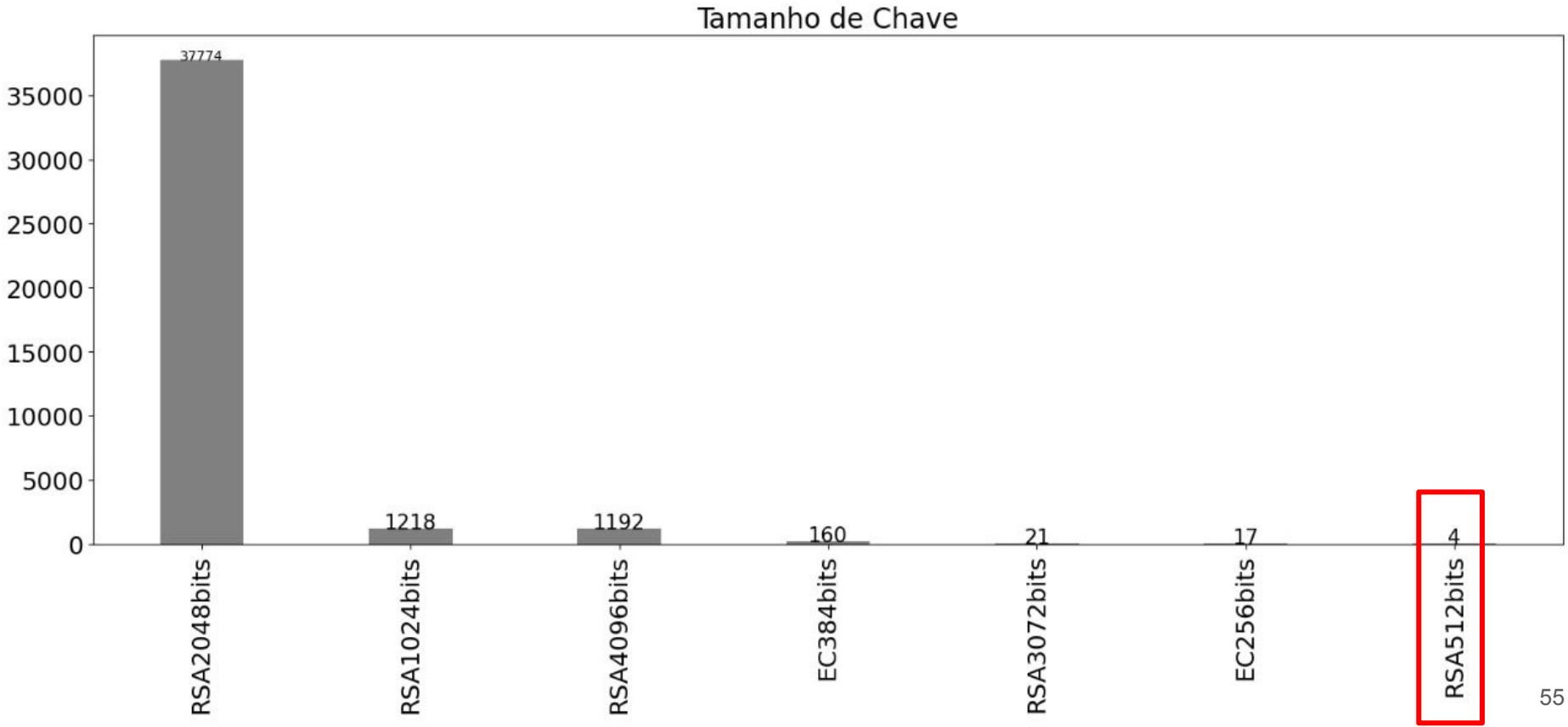
Validade do Certificado



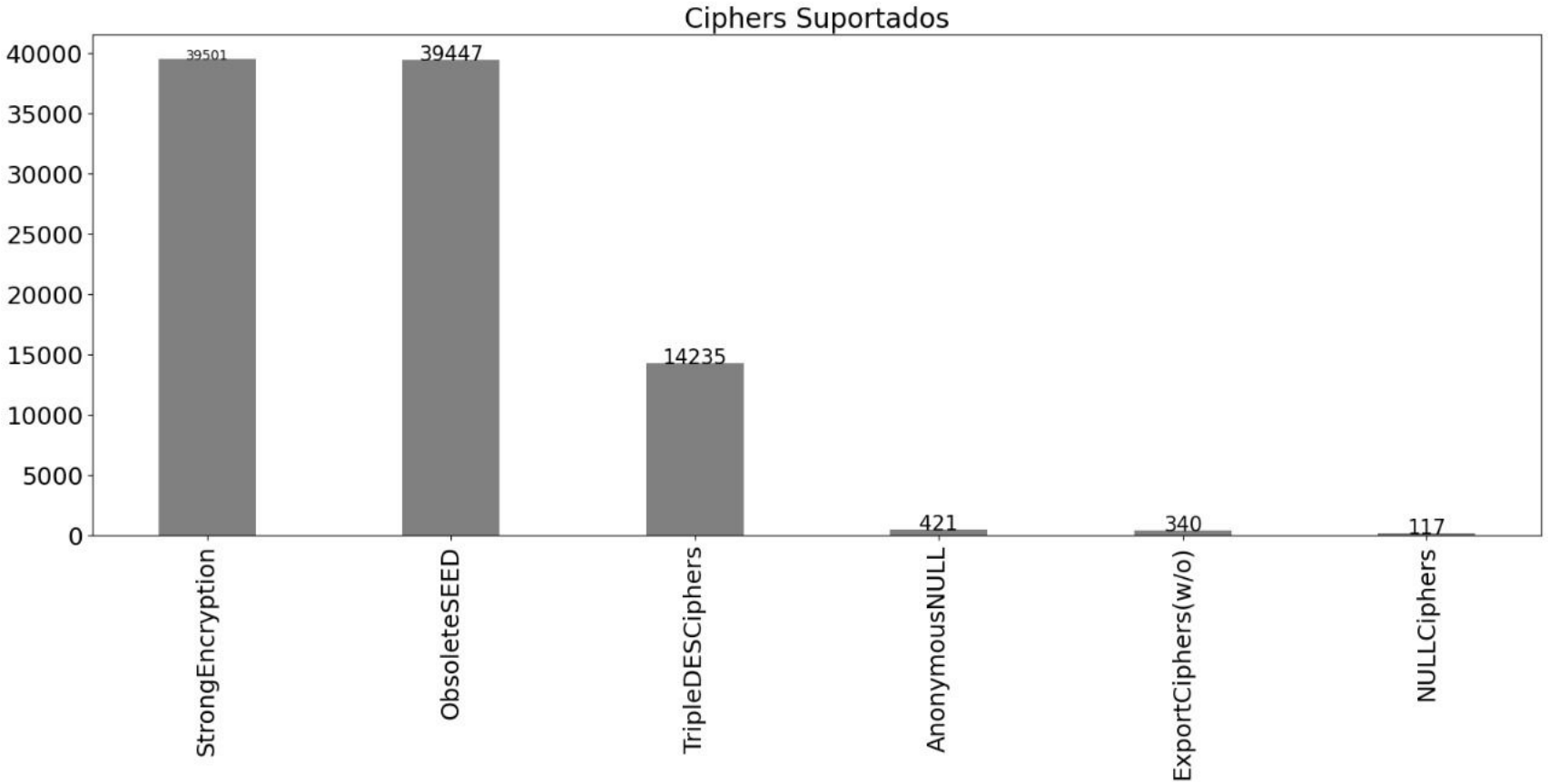
Tamanho de Chave



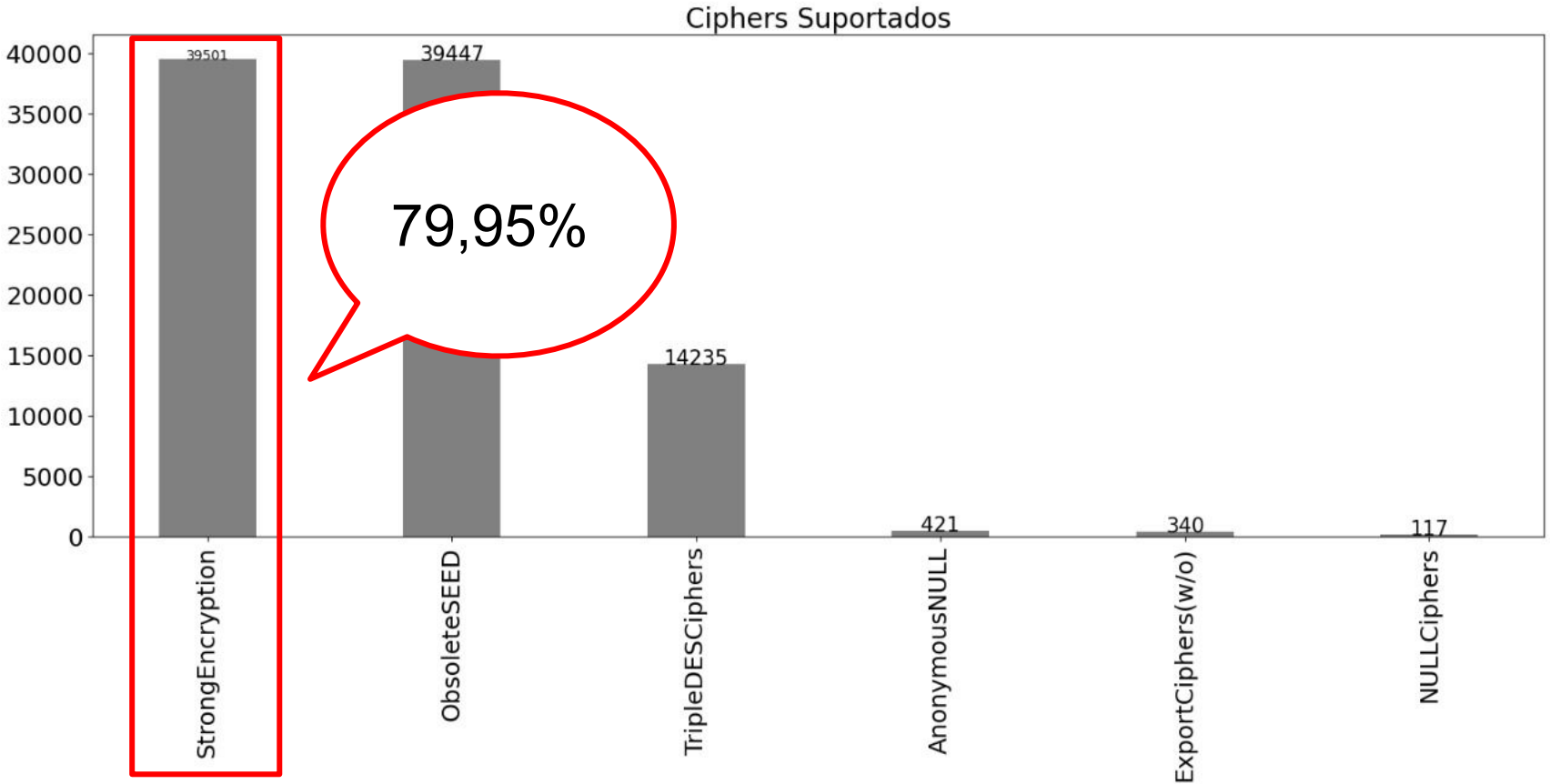
Tamanho de Chave



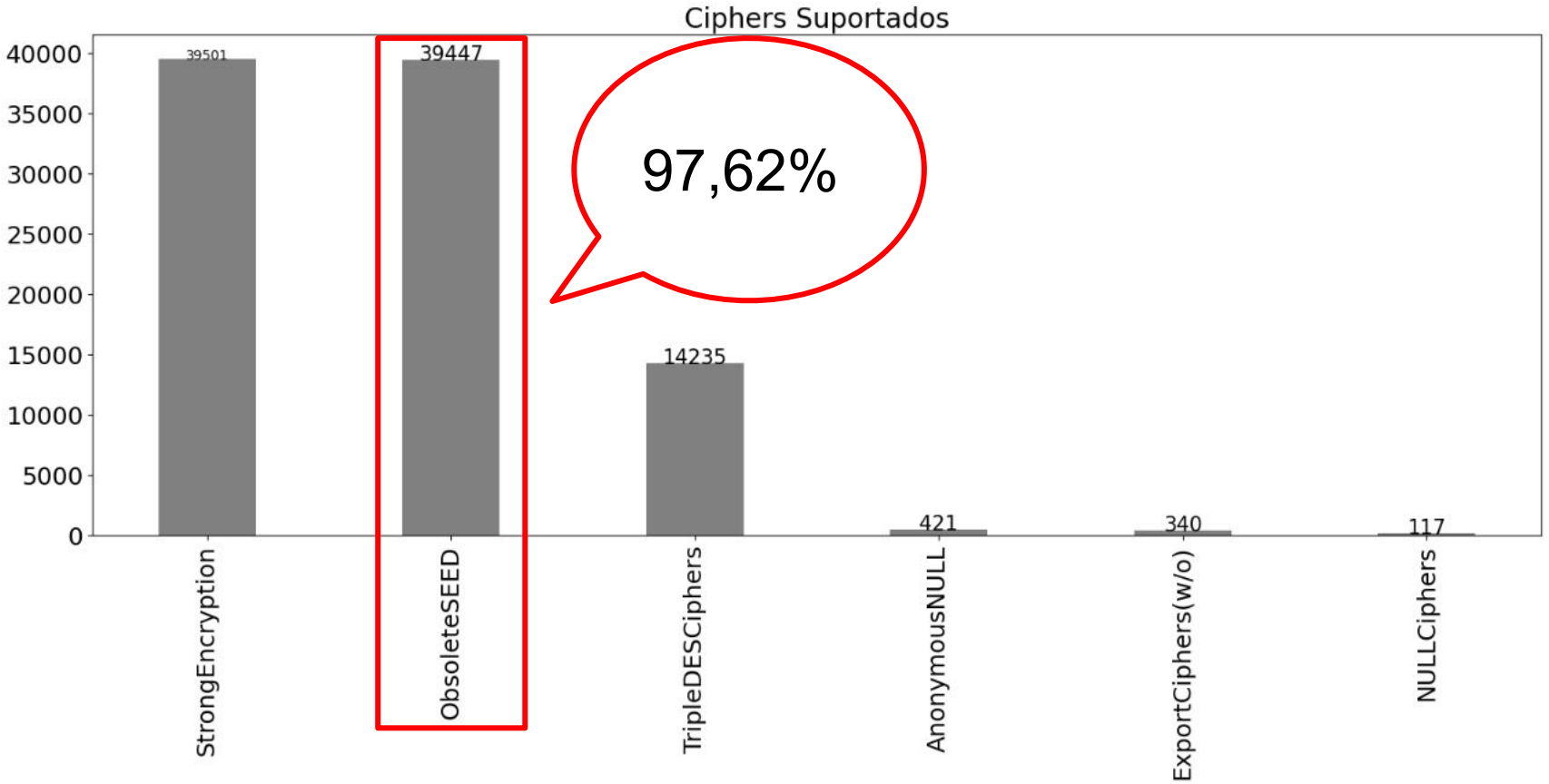
Ciphers


Ciphers Suportados
40000
35000
30000
25000
20000
15000
10000
5000
0
39501
39447
14235
421
340
117
StrongEncryption
ObsoleteSEED
TripleDESCiphers
AnonymousNULL
ExportCiphers(w/o)
NULLCiphers

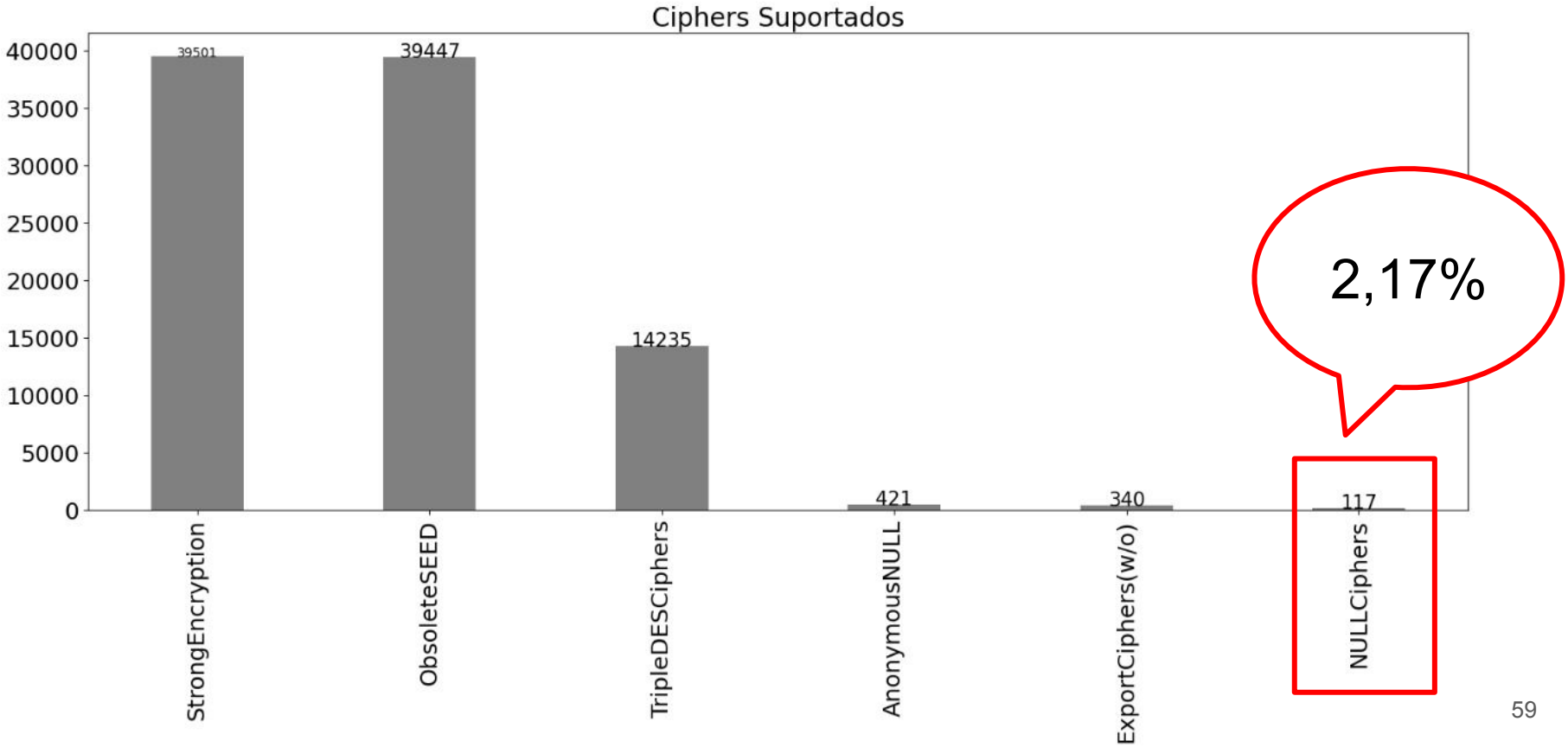
Ciphers


Ciphers Suportados
40000
35000
30000
25000
20000
15000
10000
5000
0
39501
39447
14235
421
340
117
79,95%
StrongEncryption
ObsoleteSEED
TripleDESCiphers
AnonymousNULL
ExportCiphers(w/o)
NULLCiphers

Ciphers


Ciphers Suportados
40000
35000
30000
25000
20000
15000
10000
5000
0
39501
39447
14235
421
340
117
97,62%
StrongEncryption
ObsoleteSEED
TripleDESCiphers
AnonymousNULL
ExportCiphers(w/o)
NULLCiphers

Ciphers


Ciphers Suportados
40000
35000
30000
25000
20000
15000
10000
5000
0
39501
39447
14235
421
340
117
StrongEncryption
ObsoleteSEED
TripleDESCiphers
AnonymousNULL
ExportCiphers(w/o)
NULLCiphers
2,17%

Perfect Forward Secrecy

Ano	Quantidade de Sites	Porcentagem
2020	5301	96,20%
2021	39469	97,68%

Algoritmos de Assinatura

Algoritmo de Assinatura	Quantidade de Sites	Porcentagem
RSA with SHA256	37583	93,01%
RSA with SHA1	2305	5,70%
RSA with SHA512	210	0,51%
RSA with MD5	75	0,18%
ECDSA with SHA256	19	0,04%
RSA with SHA384	10	0,02%

Algoritmos de Assinatura

Algoritmo de Assinatura	Quantidade de Sites	Porcentagem
RSA with SHA256	37583	93,01%
RSA with SHA1	2305	5,70%
RSA with SHA512	210	0,51%
RSA with MD5	75	0,18%
ECDSA with SHA256	19	0,04%
RSA with SHA384	10	0,02%

Algoritmos de Assinatura

Algoritmo de Assinatura	Quantidade de Sites	Porcentagem
RSA with SHA256	37583	93,01%
RSA with SHA1	2305	5,70%
RSA with SHA512	210	0,51%
RSA with MD5	75	0,18%
ECDSA with SHA256	19	0,04%
RSA with SHA384	10	0,02%

Roteiro

- Introdução
- Ferramentas
- Metodologia
- Resultados
- **Considerações Finais**

Considerações Finais

- 98% suportam versões inferiores a 1.3 do TLS
- 11,01% suportam a versão 1.3 do TLS
- 97,62% possuem cifras obsoletas
- 10% utilizam certificados expirados
- 15,15% quebram a cadeia do certificado

Trabalhos Futuros

- Nova varredura (em andamento)
  - Estratégias para não bloqueio:
    - randomização
    - sneaky nmap
  - Mais de 100.000 sites com HTTPS já identificados

unipampa

Universidade Federal do Pampa

Obrigada!