unipampa

Universidade Federal do Pampa

Estatísticas de 40k+ sites do Ecossistema HTTPS no Brasil

Débora Patrícia Ströher
Diego Kreutz
Rodrigo Brandão Mansilha

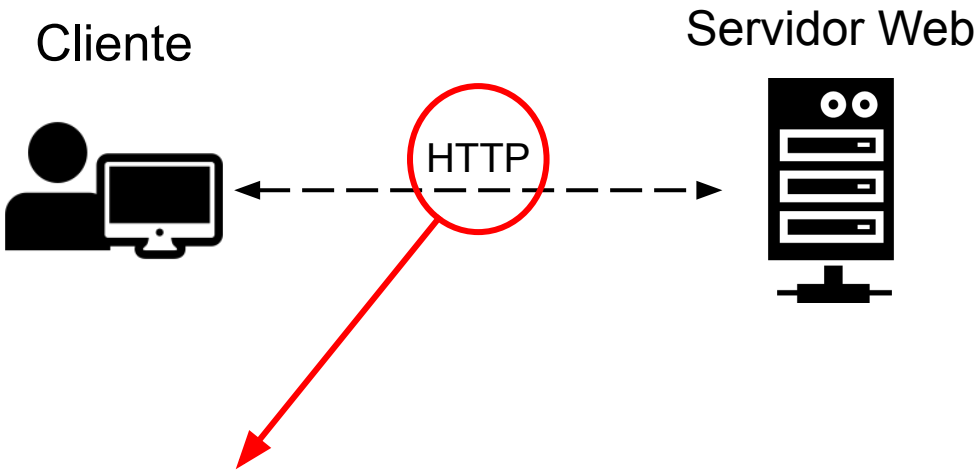
Roteiro

- Introdução
- Ferramentas
- Metodologia
- Resultados
- Considerações Finais

Roteiro

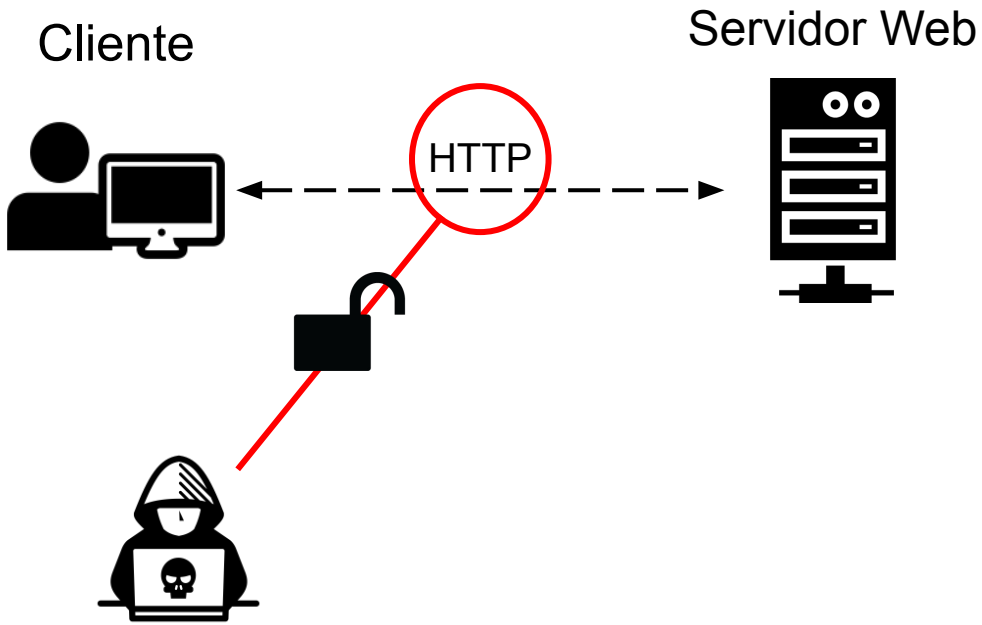
- **Introdução**
- Ferramentas
- Metodologia
- Resultados
- Considerações Finais

HTTP

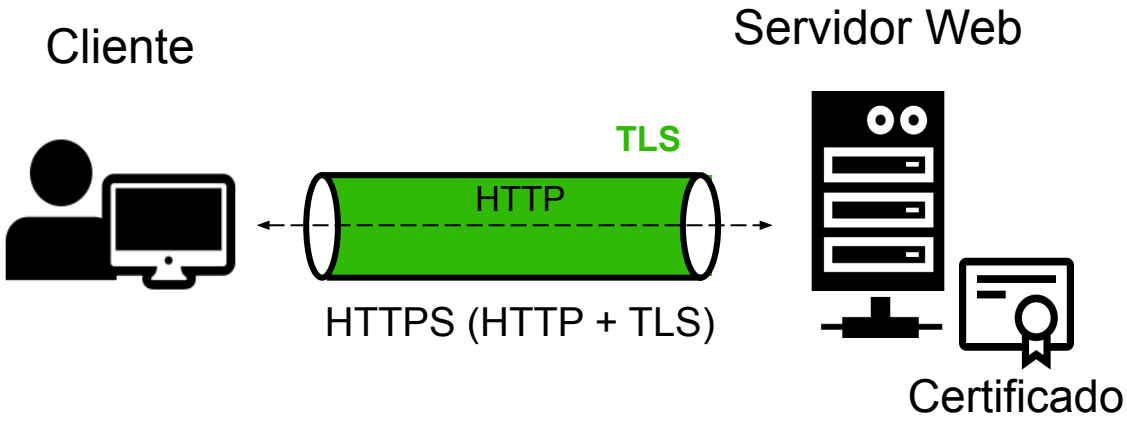


- Protocolo de Transferência de Hipertexto (HTTP)

HTTP



HTTPS



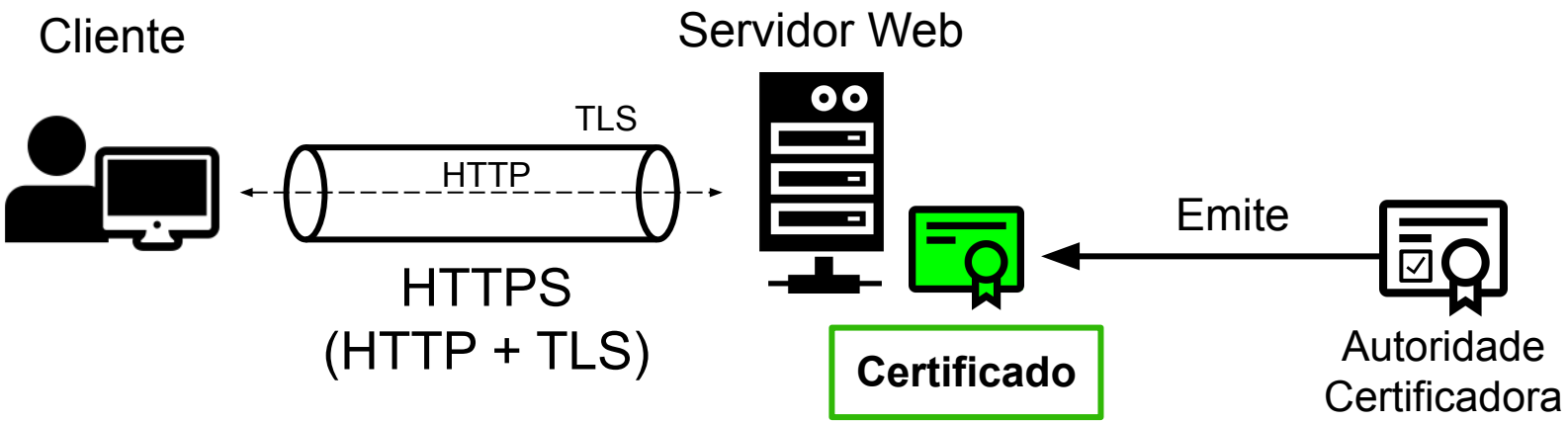
- Protocolo de transferência de hipertexto seguro (HTTPS)

SSL/TLS

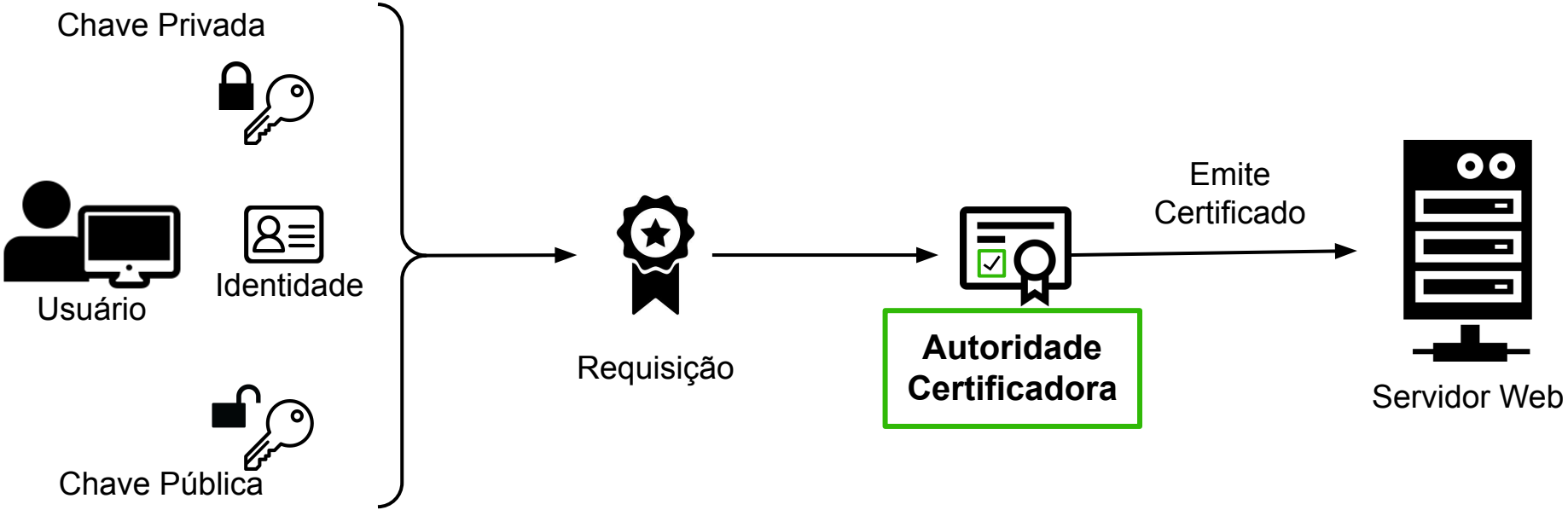
SSL/TLS

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

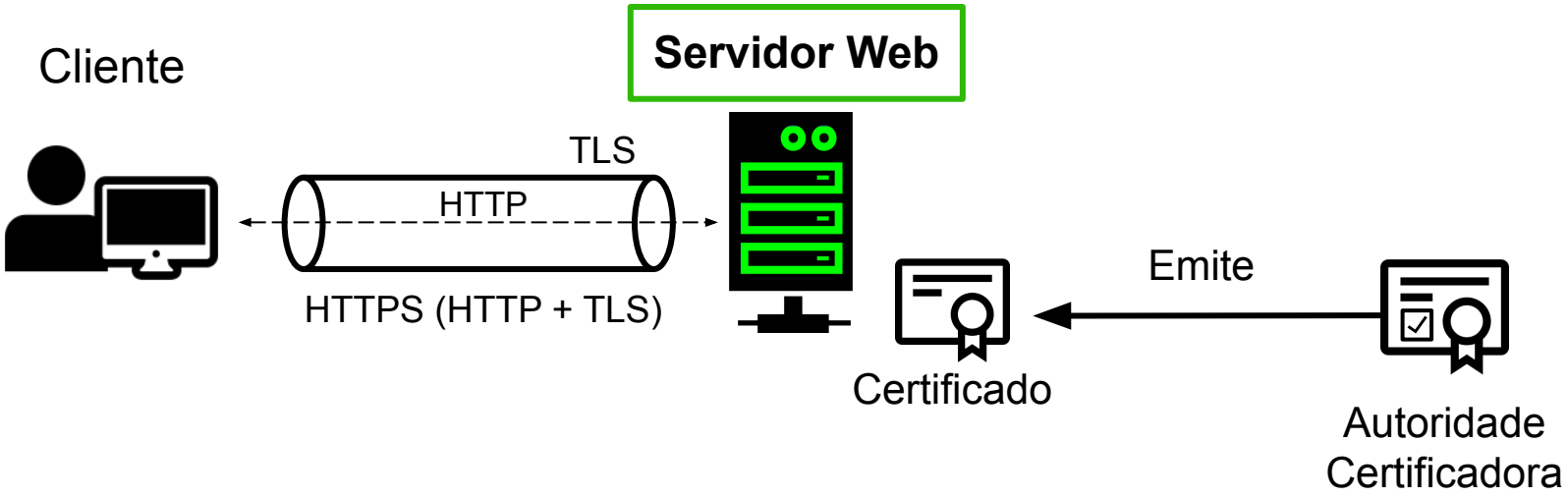
HTTPS


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

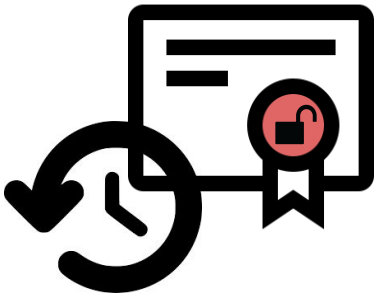
Certificado e Autoridade Certificadora



Certificados nos Servidores Web



Problemas (1/2)



- Certificados autoassinados

Problemas (2/2)

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 (2/2)

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 (2/2)

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 (2/2)

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 (2/2)

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 (2/2)

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 (2/2)

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	--	--

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 BR	5,510	**18%** implementa **incorretamente certificados digitais** **80%** ainda suportam **versões** fortemente **desaconselhadas** do SSL/TLS

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 BR	5,510	**18%** implementa **incorretamente certificados digitais** **80%** ainda suportam **versões** fortemente **desaconselhadas** do SSL/TLS

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 BR	5,510	**18%** implementa **incorretamente certificados digitais** **80%** ainda suportam **versões** fortemente **desaconselhadas** do SSL/TLS

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 BR	5,510	**18%** implementa **incorretamente certificados digitais** **80%** ainda suportam **versões** fortemente **desaconselhadas** do SSL/TLS

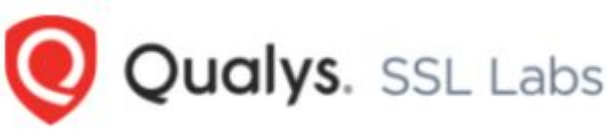
Objetivos

- 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

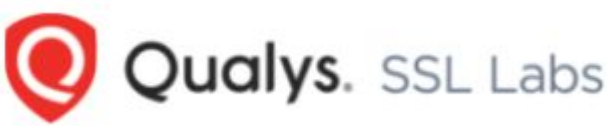
Roteiro

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

Ferramentas (navegador)



Ferramentas (navegador)



Ferramentas (terminal)

CipherScan

OpenSSL
Cryptography and SSL/TLS Toolkit

TestSSLServer

SSLyze

test SSL Testing TLS/SSL encryption

Ferramentas (terminal)

CipherScan

OpenSSL
Cryptography and SSL/TLS Toolkit

TestSSLServer

SSLyze

Testing TLS/SSL encryption

Extensões em navegadores

IndicateTLS

Certificate Pinner

Certainly Something

Extensões em navegadores

IndicateTLS

Certificate Pinner

Certainly Something

Extensões em navegadores

IndicateTLS

Certainly Something

Certificate Pinner

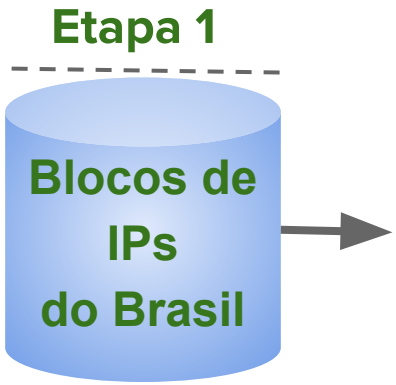
Roteiro

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

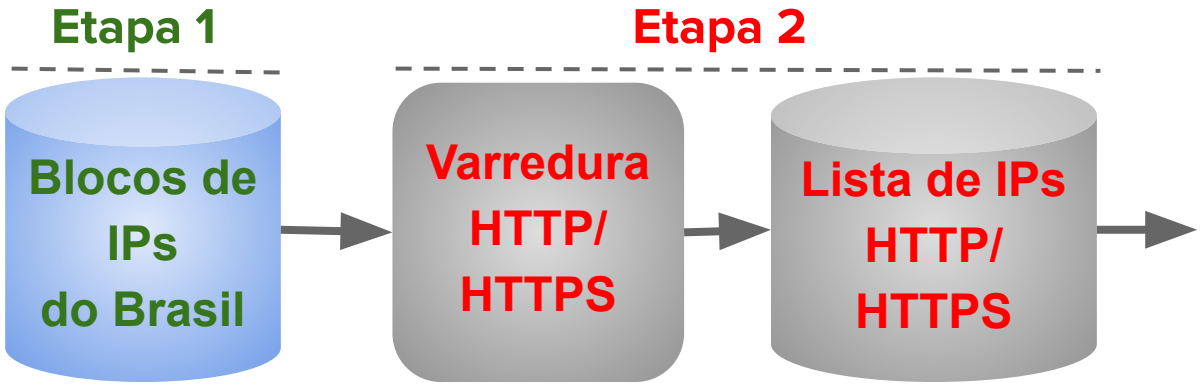
Metodologia

- Etapa 1
- Etapa 2
- Etapa 3

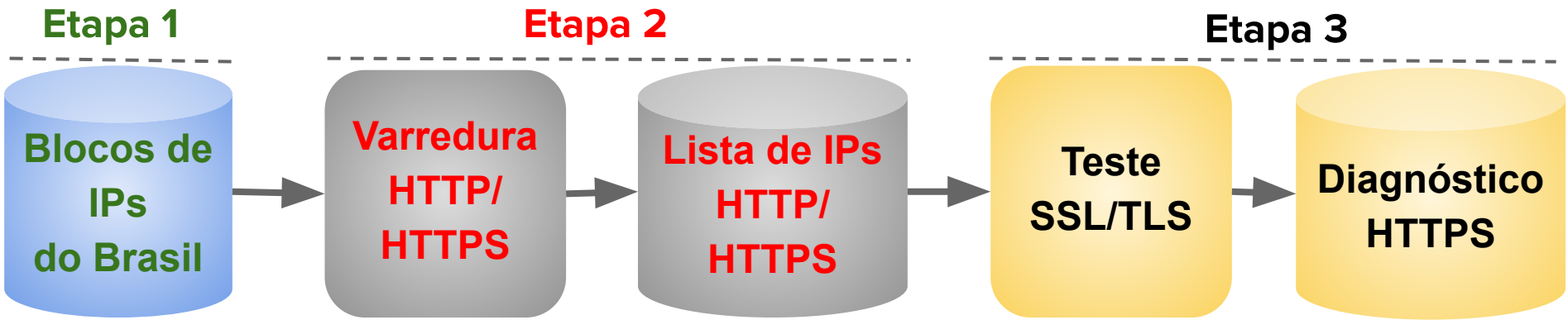
Metodologia



Metodologia



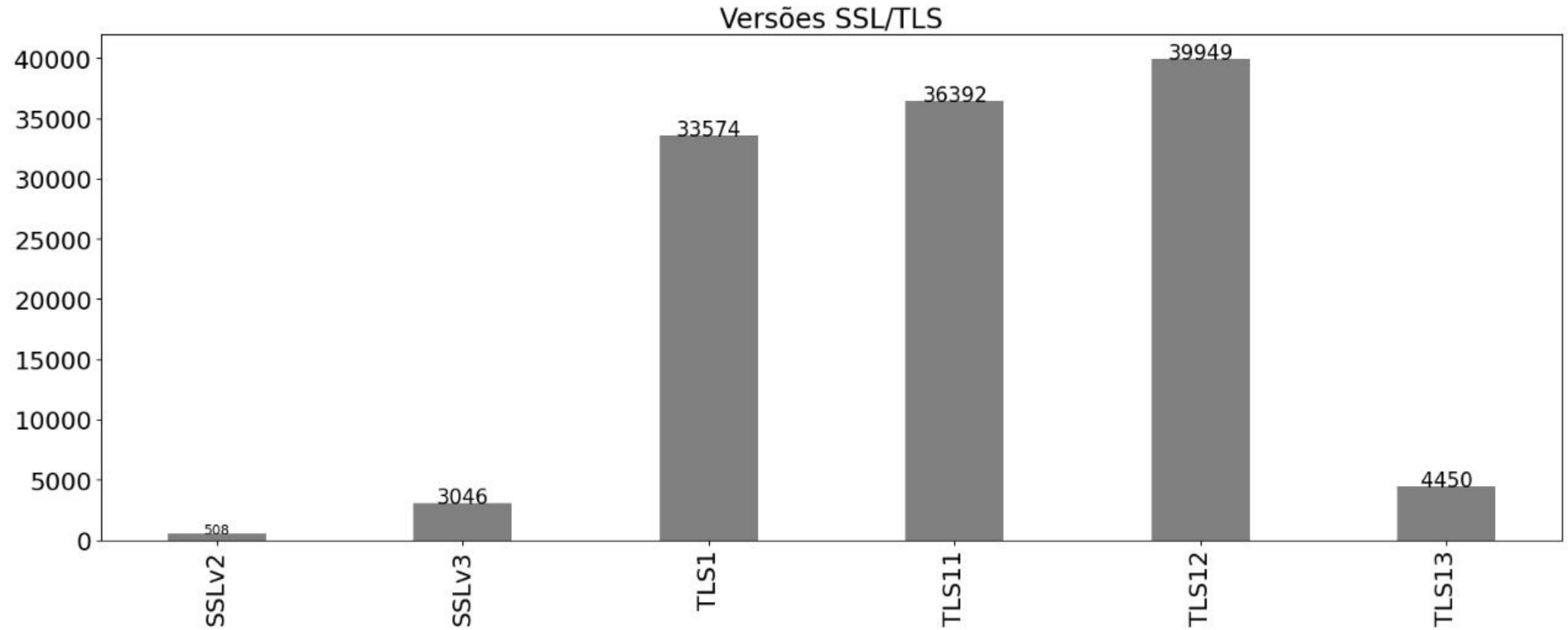
Metodologia



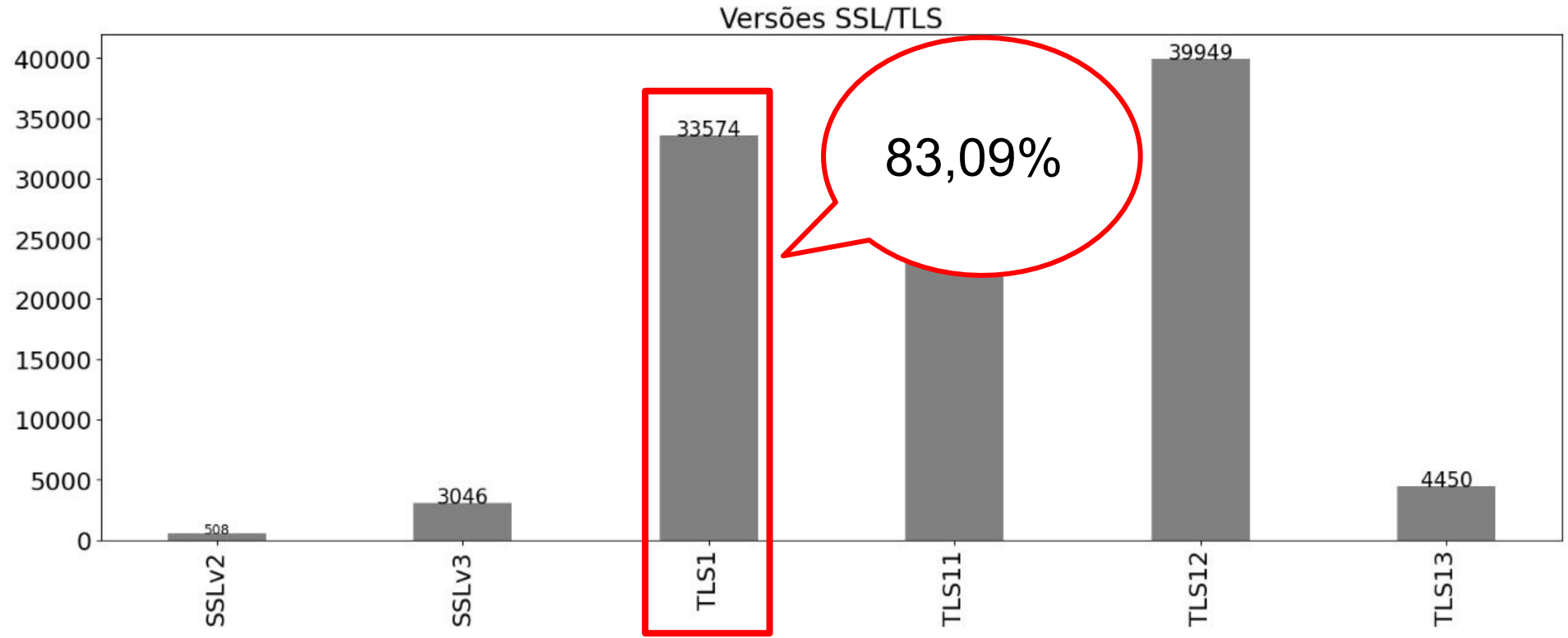
Roteiro

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

Versões dos Protocolos SSL/TLS



Versões dos Protocolos SSL/TLS



Versões dos Protocolos SSL/TLS

		1995	1996	1999	2006	2008	2018
No. 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
No. 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%

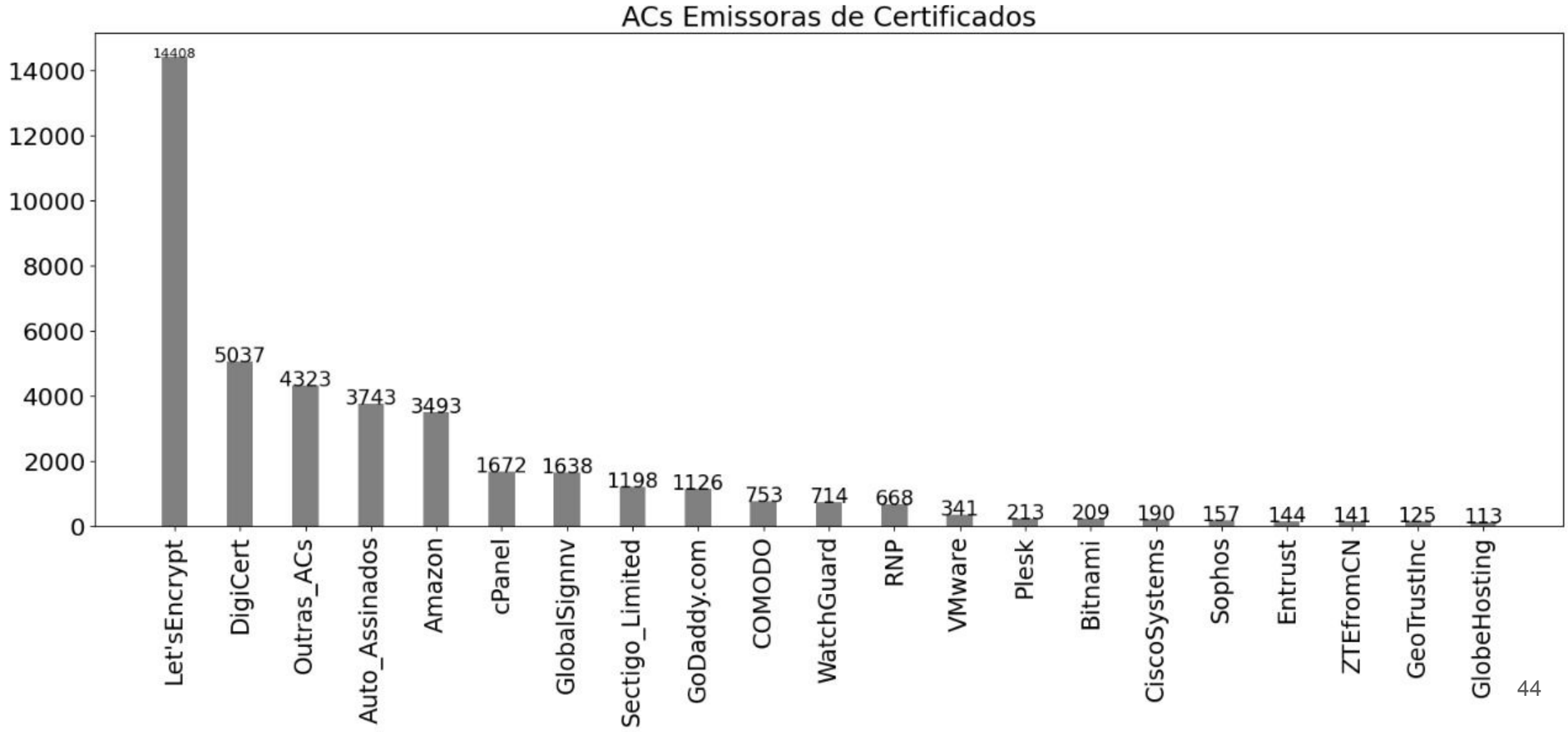
Versões dos Protocolos SSL/TLS

		1995	1996	1999	2006	2008	2018
No. 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%

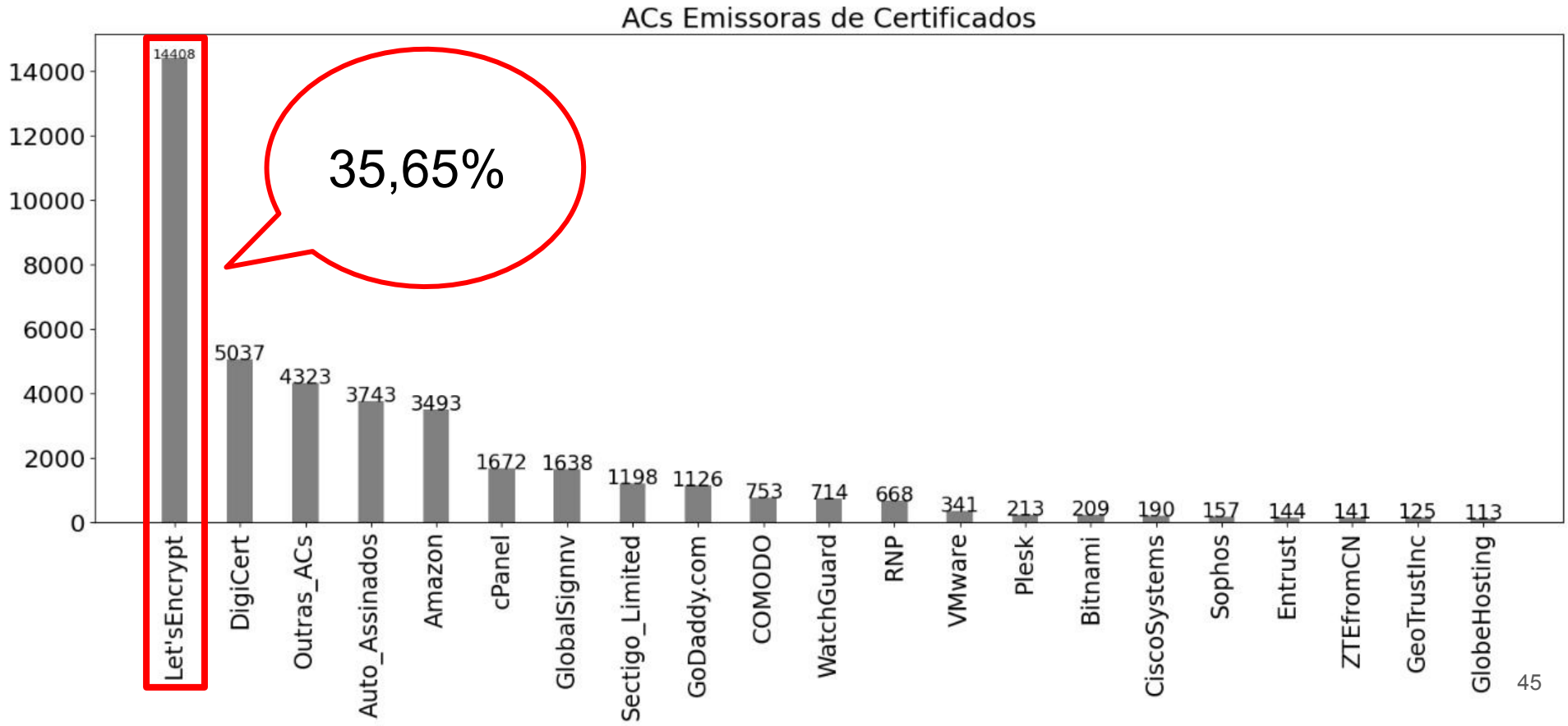
Versões dos Protocolos SSL/TLS

		1995	1996	1999	2006	2008	2018
No. 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%

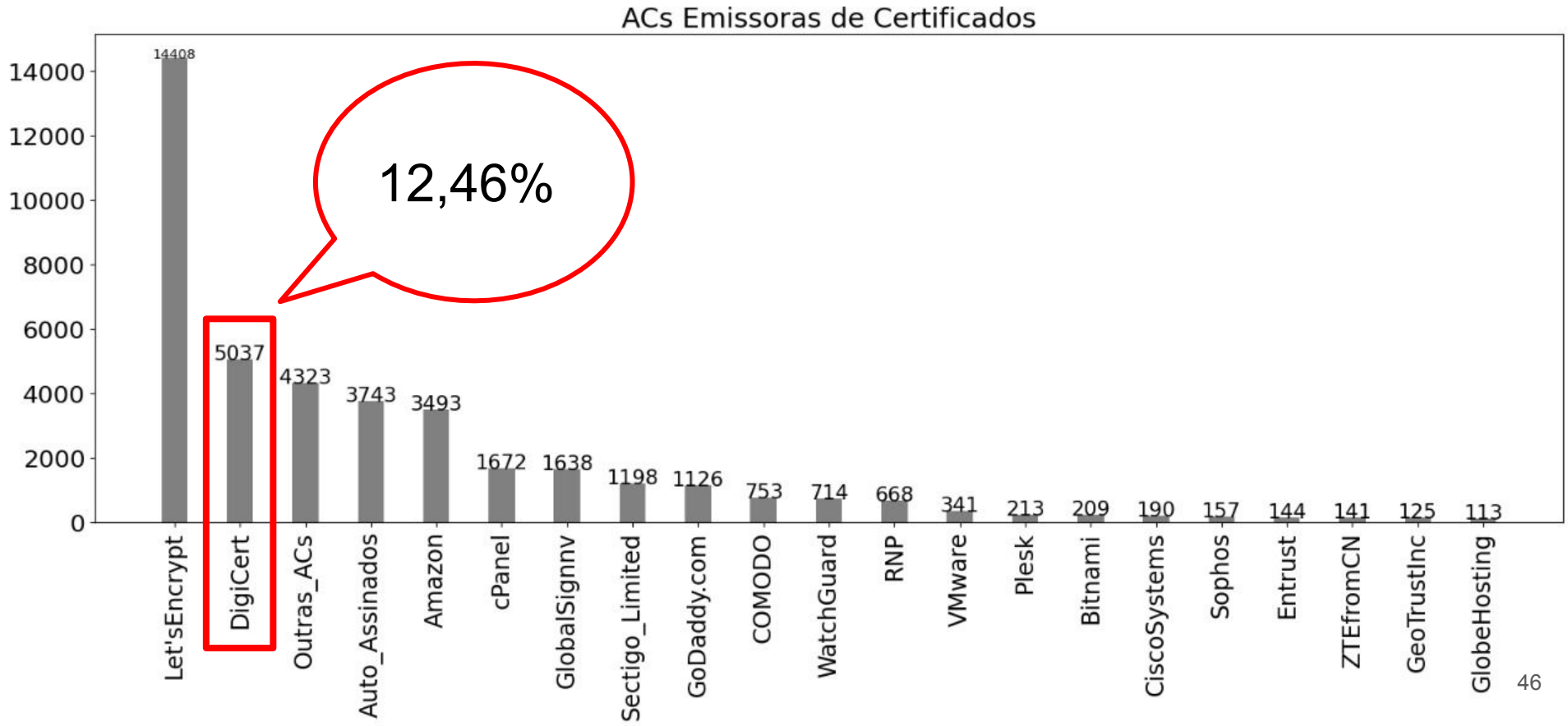
Emissores dos Certificados



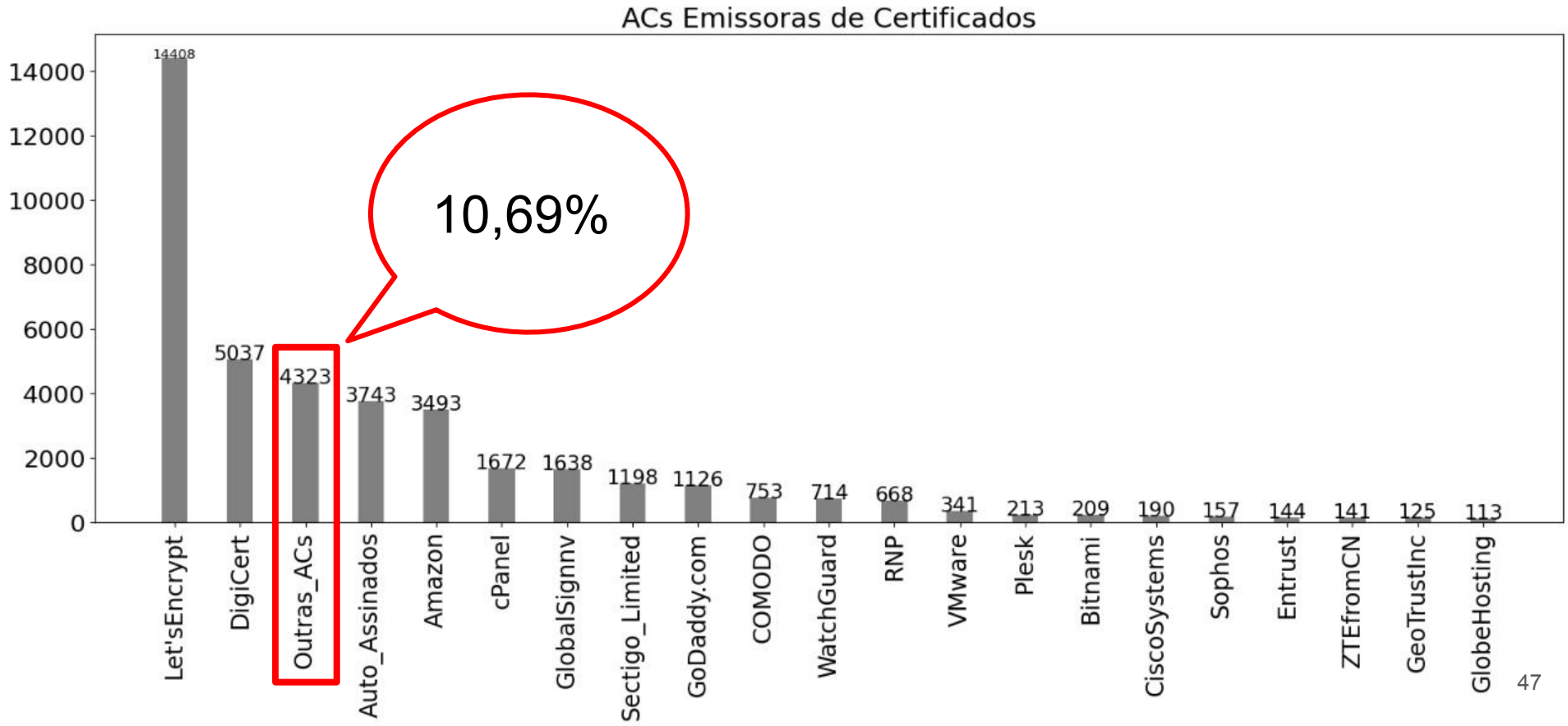
Emissores dos Certificados



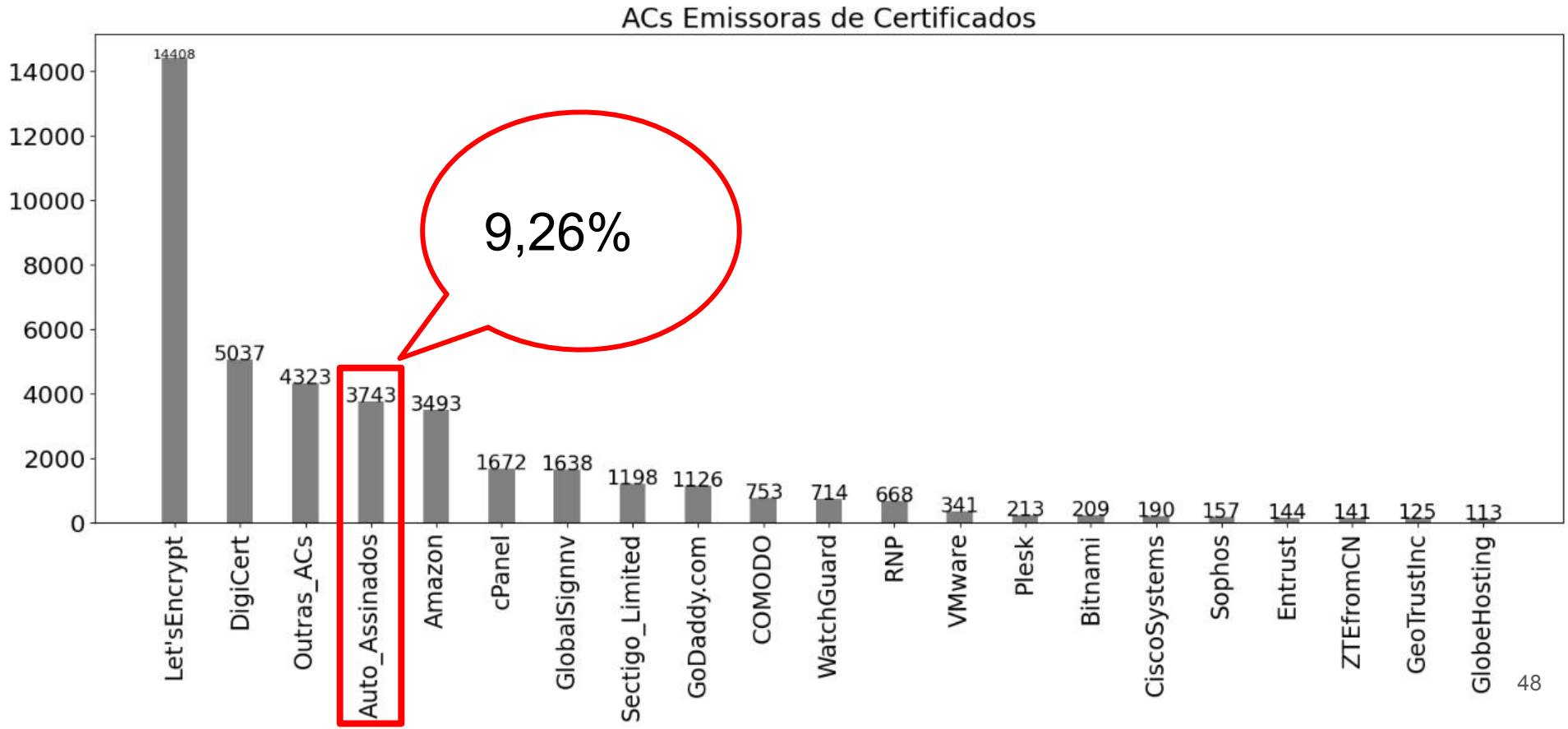
Emissores dos Certificados



Emissores dos Certificados



Emissores dos Certificados



Roteiro

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

Considerações Finais

- 40.406 sites HTTPS analisados
- 98% suportam versões inferiores a 1.3 do TLS
- 11,01% suportam a versão 1.3 do TLS
- 9,26% utilizam certificados autoassinados

Trabalhos Futuros

- Nova varredura (em andamento)
  - Estratégias para não bloqueio:
    - randomização
    - sneaky nmap
  - Mais de 150.000 sites com HTTPS já identificados

unipampa

Universidade Federal do Pampa

Obrigada!