UNIVERSIDADE FEDERAL DO PAMPA

DÉBORA PATRÍCIA STRÖHER

HTTPS no Brasil: um estudo empírico

Alegrete

2021

Débora Patrícia Ströher

HTTPS no Brasil: um estudo empírico

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Ciência da Computação da Universidade Federal do Pampa como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação.

Universidade Federal do Pampa

Orientador: Prof. Dr. Diego Kreutz

Alegrete

2021

DEBORA PATRICIA STROHER

HTTPS no Brasil: um estudo empírico

Monografia apresentada ao Curso de Ciência da Computação da Universidade Federal do Pampa, como requisito parcial para obtenção de Bacharel em Ciência da Computação.

Monografia defendida e aprovada em: 01 de outubro de 2021.

Banca examinadora:

_____

Prof. Dr. Diego Kreutz

Orientador

UNIPAMPA

_____

Prof. Dr. Rodrigo Brandão Mansilha

UNIPAMPA

Prof. Dr. Claudio Shepke

UNIPAMPA

Assinado eletronicamente por **DIEGO LUIS KREUTZ**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 01/10/2021, às 18:08, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.

Assinado eletronicamente por **CLAUDIO SCHEPKE**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 07/10/2021, às 16:50, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.

Assinado eletronicamente por **RODRIGO BRANDAO MANSILHA**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 07/10/2021, às 17:22, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.

A autenticidade deste documento pode ser conferida no site https://sei.unipampa.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0628747** e o código CRC **3A03B711**.

Agradecimentos

Agradeço à minha família por todo o apoio, paciência e compreensão, e a todos, que direta ou indiretamente, fizeram parte da minha formação.

Resumo

Estudos recentes demonstram que apenas utilizar HTTPS não garante, necessariamente, que os usuários irão navegar de forma segura no site. Neste trabalho apresentamos estatísticas de 40.406 sites HTTPS dos blocos de IPs do Brasil. Os resultados apontam que apenas 11,01% dos sites analisados suportam a versão TLS 1.3, a mais atual e a única sem vulnerabilidades conhecidas. Além disso, 9,26% utilizam certificados autoassinados, impossibilitando que um navegador o reconheça como confiável.

Palavras-chave: HTTP, HTTPS, SSL/TLS, ferramentas, vulnerabilidades,.

Abstract

Recent studies show that just using HTTPS does not necessarily guarantee that users will safely browse the site. In this work we present statistics of 40,406 HTTPS sites from IP blocks in Brazil. The results show that only 11.01% of support sites support the TLS 1.3 version, the most current and the only compliant vulnerabilities. In addition, 9.26% use self-signed certificates, making it impossible for a browser to recognize them as trusted.

Key-words: HTTP, HTTPS, SSL / TLS, tools, vulnerabilities.

Lista de figuras

Lista de tabelas

Sumário

1 Introdução

O protocolo HTTPS (*Hyper Text Transfer Protocol Secure*) é uma combinação do HTTP (*Hyper Text Transfer Protocol*) com o TLS (*Transport Layer Security*). O "S" do protocolo significa que ele oferece propriedades básicas de segurança (e.g., confidencialidade, integridade, autenticidade) às comunicações entre o cliente e o servidor web.

Estudos indicam recorrentemente que o fato de utilizar HTTPS não significa que um site oferece segurança à navegação dos usuários. Por exemplo, um estudo realizado em 2013 sobre um milhão dos sites mais populares de acordo com a classificação de Alexa Top (VRATONJIC et al., 2013) constatou que apenas 16% dos sites que implementam HTTPS utilizam certificados confiáveis, isto é, válidos e implantados adequadamente nos respectivos domínios.

Em 2019 foi publicado um estudo sobre mais de 5 milhões de sites da China (HUANG et al., 2019), no qual os autores constataram que 66,45% dos servidores web suportam apenas HTTP. Os autores identificaram também que mais de 40% dos certificados utilizam algoritmos de resumo criptográficos não recomendados (e.g., SHA1, MD5). Além disso, constataram que 49,19% dos servidores nas 10 principais regiões do país são vulneráveis ao ataque Logjam (i.e., ainda suportam a versão 1.2 do TLS).

No Brasil, um estudo publicado em 2020 (FIORENZA et al., 2020) realizou um levantamento inicial de 5.510 sites HTTPS de governos federal, estadual e municipal, comércio eletrônico e instituições financeiras. Os resultados indicam que apenas 30% dos sites suportam a versão 1.3 do TLS, mais de 92% suportam a versão 1.2 do TLS e mais de 80% ainda suportam versões fortemente desaconselhadas do SSL/TLS (e.g., TLS 1.1). O estudo também identificou que 100% dos sites oferecem riscos de segurança aos seus usuários, isto é, suportam versões vulneráveis dos protocolos SSL/TLS.

Neste trabalho, nosso objetivo é ampliar o estudo do ecossistema HTTPS do Brasil, utilizando uma amostra estatística mais representativa de sites. Para atingir o objetivo, optamos por realizar uma varredura dos blocos de IPs do Brasil. A partir de uma primeira varredura, identificamos 40.406 sites HTTPS[1].

Como contribuições deste trabalho podemos destacar: (a) um levantamento detalhado sobre ferramentas livremente disponíveis para análise de sites HTTPS; (b) uma análise mais abrangente do ecossistema HTTPS do Brasil; (c) identificação de estatísticas que apontam para um cenário bastante preocupante (e.g., apenas 11,01% dos sites

[1] O número de sites não foi maior devido a diversos problemas de bloqueio das varreduras por parte de provedores de Internet. Chegamos a receber notificações do CAIS da RNP (<https://www.rnp.br/en/sistema-rnp/cais>).

suportam a versão 1.3 do TLS).

O restante deste trabalho está organizado como segue. Na Seção 2 apresentamos alguns conceitos relacionados aos certificados de domínio. Na Seção 3 introduzimos as principais ferramentas disponíveis livremente para a análise de sites HTTPS. Nas seções 4 e 5 descrevemos a metodologia adotada no trabalho e os resultados, respectivamente. Finalmente, apresentamos as considerações finais na Seção 6. [2]

[2] Uma grande parcela do conteúdo do TCC faz parte de um artigo submetido para o WRSeg2021.

2 Certificados de Domínio

Os certificados de domínio permitem estabelecer conexões seguras (e.g., através de HTTPS) entre os clientes (e.g., navegadores) e os servidores (e.g., Web). Os certificados de domínio são emitidos por uma Autoridade Certificadora (AC), que é uma entidade da Infraestrutura de Chave Pública (ICP). As ICPs foram criadas com o objetivo de oferecer serviços (e.g., emissão e revogação de certificados) que permitem garantir propriedades de segurança essenciais aos envolvidos na comunicação, como autenticidade, integridade, confidencialidade e o não repúdio dos dados (EDUCATION, 2020). Essas propriedades são asseguradas a partir dos certificados de domínio no ecossistema HTTPS. Na prática, um navegador consegue verificar a autenticidade e confiabilidade de um site HTTPS através do seu certificado de domínio.

Na ICP, as ACs são responsáveis pela emissão, validação e revogação de certificados de domínio. Um certificado desse tipo contém informações sobre o nome do domínio (site), chave pública associada e proprietário, AC emissora e validade do certificado. Os certificados representam a base da segurança do ecossistema HTTPS (EDUCATION, 2020).

Os sistemas operacionais e navegadores possuem uma lista interna de assinaturas confiáveis, aos quais chamamos de certificados raiz. Para verificar um certificado de um site, o navegador analisa o caminho de certificação, que é uma sequência de certificados conectando a raiz da AC ao certificado do servidor (Fu et al., 2018).

Problemas de segurança associados aos certificados de domínio incluem validade (e.g., certificado expirado), nome de domínio (e.g., DNS do site diferente do nome contido no certificado), e AC emissora do certificado. Um exemplo comum relacionado ao último caso é o de certificados autoassinados, ou seja, que não possuem assinatura de uma AC conhecida e acreditada. Os certificados autoassinados levam tipicamente a custos operacionais e riscos de segurança e, por isso, devem ser evitados (KAPPENBERGER, 2012).

3 Ferramentas

Nesse trabalho é dado ênfase para ferramentas de análise de sites HTTPS de código aberto, que consigam obter informações sobre os certificados, versões dos protocolos e suas vulnerabilidades. Um mapeamento e classificação das ferramentas é apresentado Tabela 2, contendo ferramentas e suas respectivas funcionalidades divididas em categorias. Para usuários leigos ferramentas como SSL Labs, SSL Checker, ImmuniWeb e Digicert são mais simples de utilizar, já que funcionam pelo navegador e possuem uma interface mais amigável, algumas delas trazendo uma **Classificação** da qualidade de segurança do site. Para usuários mais avançados que precisam analisar um conjunto grande de sites, ferramentas como Cipherscan, TestSSLServer, SSLyze e testssl.sh são mais recomendadas.

Em **Informações do Certificado** podemos analisar informações sobre a AC emissora, a validade e o domínio do certificado. Dentre as ferramentas, apenas SSL Labs, SSL Checker, ImmuniWeb, Digicert, Observatory e testssl.sh recuperam todas as informações sobre certificados. As restantes apresentam de maneira limitada ou até mesmo não apresentam essas informações.

Em **Protocolo** podemos identificar quais ferramentas retornam informações sobre as versões de protocolos suportadas e vulnerabilidades conhecidas para os mesmos. A Cadeia do certificado permite identificar se um certificado é confiável ou não. Certificados ditos como confiáveis possuem uma validade, são emitidos por uma AC emissora e possuem AC raíz.

Tabela 1 – Ferramentas de análise de sites HTTPS

	Modo de operação		**Informações do certificado**				**Protocolo**		**Classificação**
Ferramenta	Navegador	Terminal	Emissor	Validade	Domínio	Cadeia do certificado	Versão	Vulnerabilidades	Possui
SSL Labs	x		x	x	x	x	x	x	x
ImmuniWeb	x		x	x	x	x	x	x	x
Digicert	x		x	x	x	x	x	x	
Observatory	x		x	x	x		x		x
SSL Checker	x		x	x	x				
Wormly	x			x	x		x		x
pentest-tools	x						x	x	x
CryptCheck	x						x		x
Geekflare TLS Scanner	x						x		
Cipherscan		x					x		
TestSSLServer		x	x				x		
SSLyze		x					x	x	
OpenSSL		x	x			x	x		
testssl.sh		x	x	x	x	x	x	x	
Extensão Navegador									
IndicateTLS	x		x	x	x		x		
Certainly Something	x		x	x	x		x		
Certificate Pinner	x			x					

Adaptado de (FIORENZA et al., 2020)

O conjunto das três primeiras ferramentas, SSL Labs, ImunniWeb e Digicert, retornam todas as informações sobre certificado apontadas na tabela, juntamente com as

informações dos protocolos. Já as três subsequentes, Observatory, SSL Checker e Wormly, apresentam um conjunto reduzido dessas informações, seja não apresentando emissor, cadeia ou até mesmo versões dos protocolos. As três últimas ferramentas que possuem modo de operação via navegador, pentest-tools, CryptCheck e Geekflare TLS Scanner, não trazem nenhuma informação sobre o certificado, apenas informações sobre versão e vulnerabilidades dos protocolos .

4 Metodologia

A Figura 1 resume o processo adotado para a coleta e análise dos dados. Na primeira etapa foram coletados os dados referentes aos blocos de IPs do Brasil, utilizando a lista de 2.286 blocos de IPs da NirSoft (<https://www.nirsoft.net/countryip/br.html>). A partir desses blocos geramos as sequências de mais de 77 milhões de IPs.

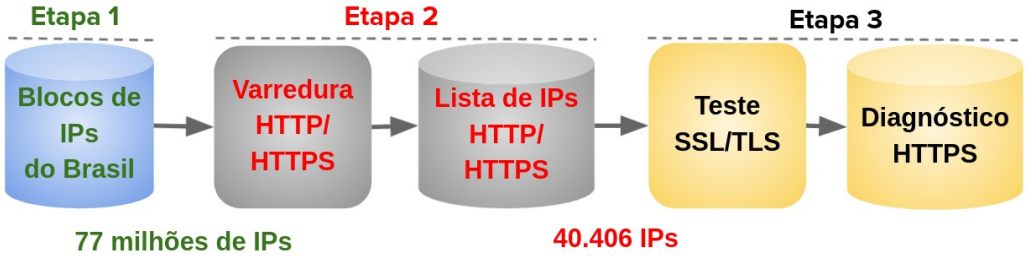

Figura 1 – Processo de coleta e análise dos dados

Na segunda etapa realizamos a varredura dos IPs em busca de conexões HTTP ou HTTPS. Para identificar portas com HTTP ou HTTPS habilitado, utilizamos a ferramenta `wget` (<https://www.gnu.org/software/wget/>) do Linux. Ao final dessa etapa, identificamos mais de 40 mil sites com HTTPS habilitado. É importante destacar que diversos provedores de Internet acabaram por bloquear nossas varreduras, pois interpretaram as requisições aos IPs dos respectivos blocos como varreduras pré-ataque. Sem os bloqueios certamente aumentaríamos o número de IPs identificados com HTTPS habilitado.

Na terceira etapa realizamos o teste da conexão HTTPS dos IPs identificados na etapa anterior. Para automatizar a análise, utilizamos a ferramenta `testssl.sh` (<https://testssl.sh/>), que identifica as versões dos protocolos SSL/TLS suportadas pelos sites, bem como extrai informações detalhadas sobre os certificados do domínio.

5 Resultados

As saídas da ferramenta `testssl.sh`, para os 40.406 sites, estão disponíveis no GitHub (<https://github.com/HTTPS-TLS-BR/WRSeg21>). Para cada endereço IP há um arquivo contendo os dados completos de saída dos testes da ferramenta, incluindo informações associadas aos certificados, algoritmos de assinatura, tamanhos de chaves, versões e vulnerabilidades associadas aos protocolos. Esta seção está organizada em 8 subseções, como segue:

- **Seção 5.1**: resumo sobre as versões dos protocolos suportadas pelos sites. É interessante destacar que apenas 11,05% dos sites suportam o TLS na versão 1.3.
- **Seção 5.2**: informações sobre os emissores dos certificados. Destes podemos destacar que 9,26% apresentaram certificados autoassinados.
- **Seção 5.3**: dados sobre a cadeia de confiança, onde apenas 68,92% possuem a cadeia completa.
- **Seção 5.4**: estatísticas sobre a validade do certificado. A quantidade de sites que apresentaram certificados expirados chegou a quase 10%.
- **Seção 5.5**: informações sobre o tamanho de chave a princípio não obtiveram problemas, pois 99,94% utilizam padrões RSA e EDCDA recomendados.
- **Seção 5.6**: dados sobre os ciphers apontaram que 97,62% possuem suporte à cifras obsoletas, ou seja, possuem um ou mais mecanismos fracos.
- **Seção 5.7**: traz um resumo sobre o Perfect Forward Secrecy. A princípio também não obteve problemas pois 97,68% dos sites oferecem suporte ao PFS.
- **Seção 5.8**: algoritmos de assinatura 5,89% dos sites ainda utilizam algoritmos de assinatura obsoletos, como MD5 e SHA1.

5.1 Versões dos Protocolos SSL/TLS

Na Figura 2 apresentamos as diferentes versões dos protocolos SSL/TLS suportadas pelos sites. A soma dos valores das versões ultrapassa o número total de sites porque um site pode suportar múltiplas versões. Como podemos observar, 90,06% dos sites ainda suportam TLS 1.1, o que é um dado preocupante devido ao fato de que essa versão do protocolo ser fortemente desaconselhada desde 2008. Ainda mais preocupante é o fato de mais de 83% dos sites ainda suportarem a versão 1.0 do TLS, que deveria estar em desuso

desde 2006. Isso significa que uma grande parcela dos sites HTTPS ainda continua colocando usuários em risco através de ataques conhecidos e bem documentados na Internet, como BEAST, POODLE e Logjam.

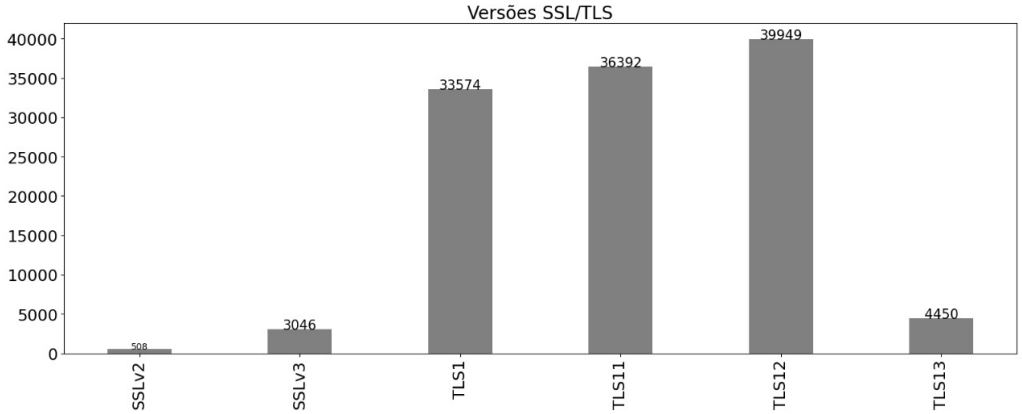

Figura 2 – Versões dos Protolos SSL/TLS

Outro aspecto preocupante é o baixíssimo número de sites que suportam o TLS 1.3 (apenas 11,01%). Desde 2018, utilizar TLS 1.3 é o método mais eficaz para mitigar diferentes vulnerabilidades e ataques de versões anteriores do protocolo. Entretanto, a maioria absoluta dos servidores Web ainda não suporta essa versão do protocolo. Consequentemente, mesmo que os navegadores dos usuários estejam atualizados, não será possível estabelecer uma conexão TLS 1.3 com os sites HTTPS.

Na Tabela 2 apresentamos os resultados de (FIORENZA et al., 2020) (5.510 sites HTTPS) e os nossos resultados para os 40.406 sites HTTPS. O dado que mais chama atenção é a porcentagem de sites que suportam o TLS 1.3. Num escopo mais limitado, chegou a 31,83% dos sites, entretanto, em uma análise mais abrangente (e.g., incluindo sites de diversos setores, como hotelaria e sustentabilidade), esse número reduziu para apenas 11,01%. Isso significa que o cenário é ainda mais preocupante do que o imaginado anteriormente.

Tabela 2 – Resultados em perspectiva versões TLS/SSL

Quantidade de sites	Ano	SSLv2	SSLv3	TLS 1	TLS 1.1	TLS 1.2	TLS 1.3
5.510	2020	1,92%	5,26%	76,17%	80,09%	97,35%	31,83%
40.406	2021	1,25%	7,53%	83,09%	90,06%	98,86%	11,01%

5.2 Emissores dos Certificados

Na análise dos dados, identificamos mais de 4.300 ACs emissoras dos certificados. Devido a esse valor ser consideravelmente grande, decidimos apresentar as 18 ACs mais

frequentemente utilizadas, o número de certificados autoassinados e o números total de outras ACs na Figura 3.

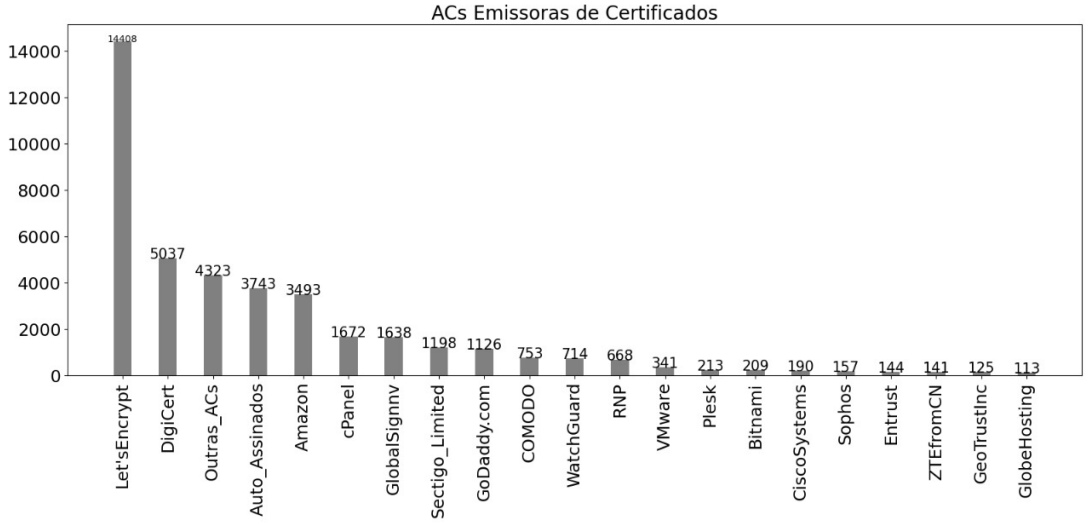

Figura 3 – ACs Emissores de Certificados

A Let's Encrypt é a AC mais utilizada, representando uma fatia de 35,65% dos sites analisados. A segunda colocada é a AC comercial DigiCert, responsável pelos certificados de 12,46% dos sites. Como podemos perceber, os certificados autoassinados aparecem em terceiro lugar, perfazendo 9,26% do total, chegando muito próximo ao somatório de todas as demais ACs não representadas no gráfico. Esses números indicam que há uma tendência crescente por ACs gratuitas, como é o caso da Let's Encrypt. Mesmo com certificados que precisam ser renovados a cada 3 meses, a utilização desta AC vem claramente ganhando espaço no mercado.

5.3 Cadeia de Confiança

O gráfico 4 mostra os dados sobre a cadeia de confiança do certificado. Podemos constatar que 68,92% possuem a cadeia completa. Em contrapartida 15,15% deles quebram a cadeia do certificado pois possuem uma AC autoassinada na cadeia, ou seja, a empresa que o emite também assina. E ainda 11,13% possuem a cadeia do certificado quebrada, impedindo que um navegador o reconheça como confiável.

Os resultados na barra "Inválida"dizem respeito às saídas contendo algum erro, ou seja, quando a ferramenta não conseguiu reconhecer informações sobre a cadeia de confiança.

Na Tabela 3 podemos ver uma comparação dos resultados deste trabalho com o trabalho (FIORENZA et al., 2020). A diferença mais expressiva é nos valores de certificados autoassinados, chegando a um aumento de quase 10%.

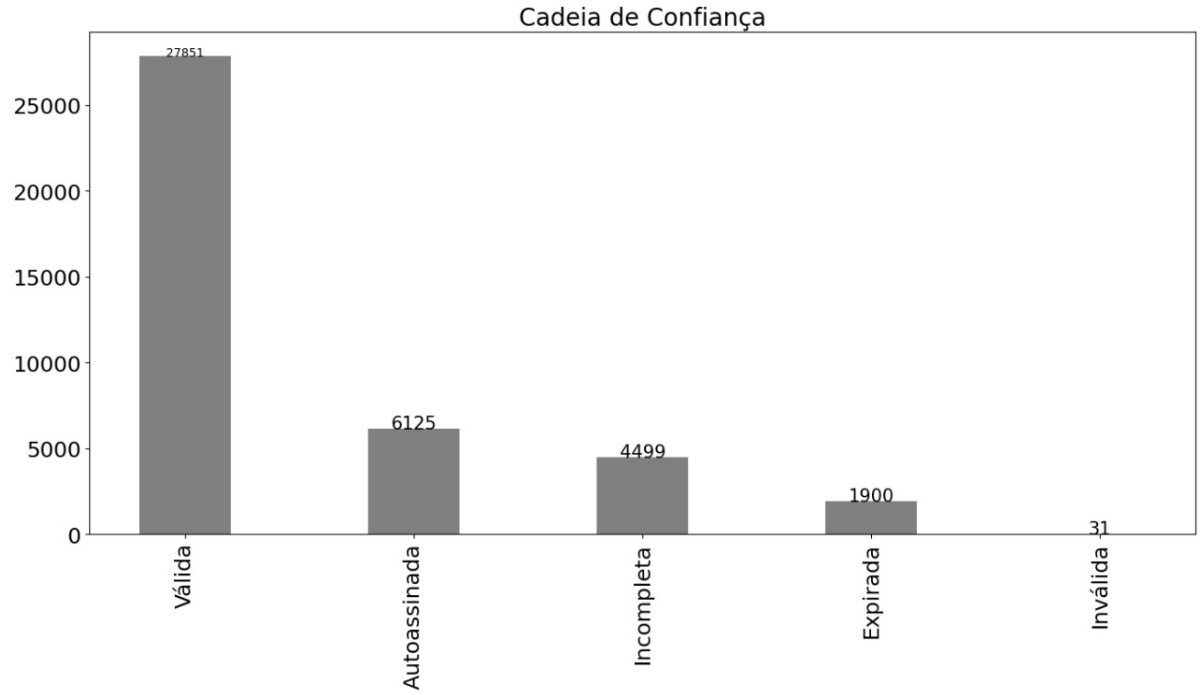

Figura 4 – Cadeia de Confiança

Tabela 3 – Resultados em perspectiva cadeia de confiança

Quantidade de sites	Ano	Incompleta	Autoassinada	Expirada
5.510	2020	12,83%	5,49%	4,22%
40.406	2021	11,13%	15,15%	4,70%

5.4 Validade do Certificado

No gráfico 5 demonstramos dados sobre a validade do certificado. As informações são apresentadas através de de intervalos de tempo, podendo ser maior ou igual a 60 ou 30 dias, ou menores que 60, 30 e 15 dias. Foi identificado que 51,11% dos certificados irão expirar em um tempo maior ou igual à 60 dias, e 32,26% em um tempo maior ou igual a 30 dias.

Os valores que expiram em menos de 60, 30 ou 15 dias representam 6,35% dos certificados. Um fator preocupante é que a quantidade de sites que apresentaram certificados expirados chegou a quase 10%. Isso é um problema grave de segurança pois tanto os sites quanto os usuários ficam suscetíveis a ataques de invasores e, em decorrência disso, são exibidos avisos nos navegadores de que o site não está seguro e apenas irá continuar se o usuário assim decidir.

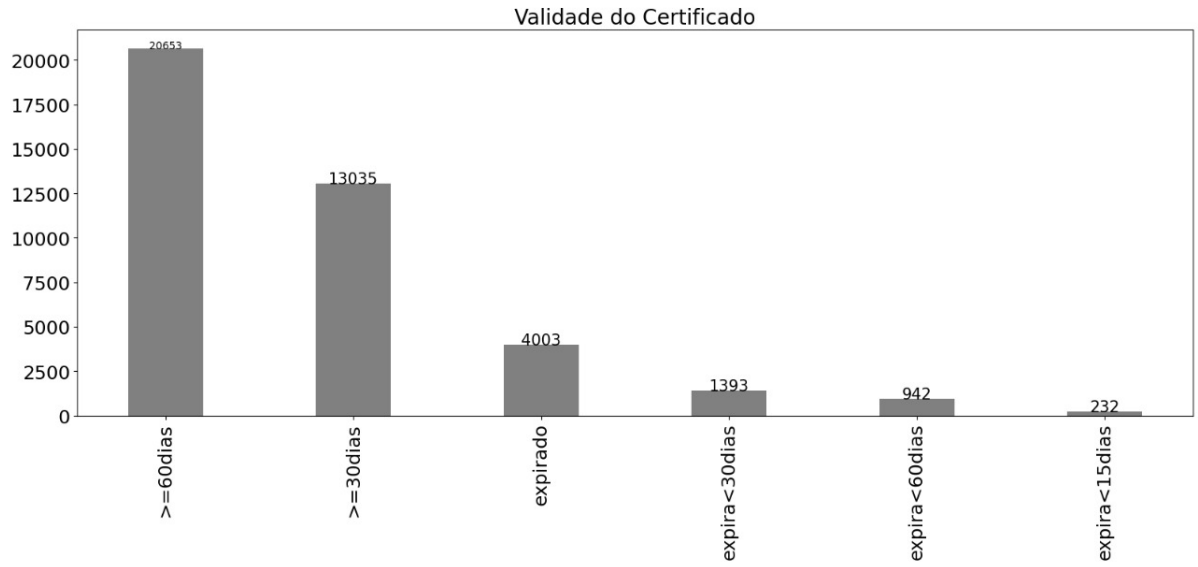

Figura 5 – Validade do Certificado

5.5 Tamanho de Chave

Quanto ao tamanho das chaves podemos analisar na Tabela 4 que 93,48% dos sites utilizam chaves RSA 2048-bit, que atualmente oferecem melhor combinação de segurança e desempenho. E ainda 0,43% utilizam EDCDA dentro dos padrões recomendados.

Tabela 4 – Tamanho de chave

Chaves	Quantidade de Sites	Porcentagem
RSA2048	37774	93,48%
RSA1024	1218	3,01%
RSA4096	1192	2,95%
EC384	160	0,39%
RSA3072	21	0,05%
EC256	17	0,04%
RSA512	4	0,009%

Apenas 4 sites utilizam padrões fracos de chave RSA, como a de 512 bits. Os valores são menores do que a quantidade total analisada pois 15 sites não obtiveram a saída esperada e 5 sites não obtiveram saída nenhuma sobre o tamanho de chave.

5.6 Ciphers

A ferramentas `testssl.sh` mostra categorias de cifras padrão para dar uma ideia inicial dos tipos de cifras suportadas. Conjuntos de criptografia consistem em um algoritmo de criptografia, um mecanismo de autenticação, um algoritmo de troca de chave e um mecanismo de derivação de chave. No gráfico 6 podemos ver que o valor total de

ciphers obtidos foi 94.061, isso se dá pelo fato de que um site pode suportar mais de um cipher. Destes, 79,95% dos sites suportam cifras fortes e recomendadas, como AEAD.

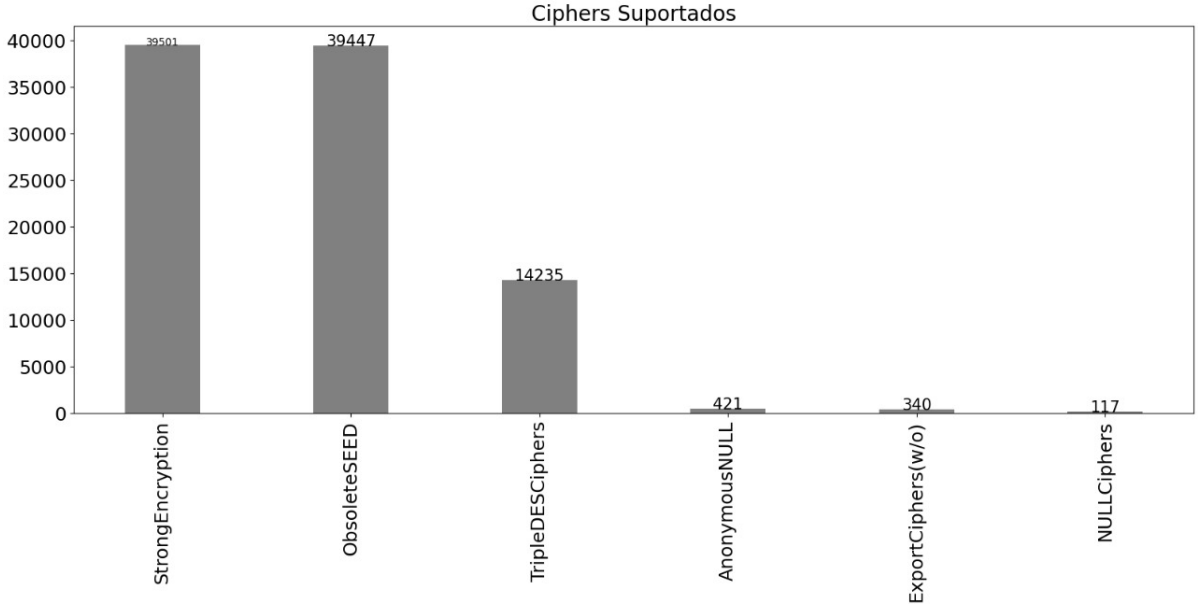

Figura 6 – Ciphers

Por outro lado, 97,62% possuem cifras obsoletas, ou seja, possuem um ou mais dos mecanismos fracos. E ainda 2,17% desses sites não possuem nenhuma criptografia, autenticação ou utilizam cifras de exportação.

5.7 Perfect Forward Secrecy

O PFS é um recurso do SSL/TLS que impede que os dados de sessões do histórico ou futuras sejam descriptografados se um invasor tiver acesso as chaves privadas utilizadas na sessão. Isso é possível através da utilização de chaves de sessão geradas exclusivamente para cada sessão (VOJTKO, 2020). Na Tabela 5 abaixo podemos verificar que 97,68% dos sites oferecem suporte ao PFS.

Tabela 5 – PFS

PFS	Quantidade de Sites
Oferece	39469
Não Oferece	937

Em comparação com o trabalho anterior (FIORENZA et al., 2020), podemos verificar na Tabela 6 que os valores não diferem muito dos encontrados no primeiro trabalho, com uma ligeira queda em sites que não oferecem.

Tabela 6 – Resultados em Perspectiva PFS

PFS	Ano	Quantidade de Sites	Porcentagem
Oferece	2020	5.301	96,2%
Oferece	2021	39.469	97,68%
Não Oferece	2020	209	3,79%
Não oferece	2021	937	2,31%

5.8 Algoritmos de Assinatura

Os algoritmos de assinatura garantem maior segurança criptográfica em transmissão de dados entre um cliente e o servidor. Existem dois algoritmos que são utilizados, o RSA (*Rivest, Shamir, and Adelman*), sendo o mais utilizado na grande maioria dos certificados, e o EDCDA (*Elliptic Curve Digital Signature Algorithm*). Na Tabela 7 podemos visualizar os algoritmos de assinatura suportados pelos sites.

Tabela 7 – Algoritmos de Assinatura

Algoritmo de Assinatura	Quantidade de Sites	Porcentagem
RSA with SHA256	37.583	93,01%
RSA with SHA1	2.305	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%

Em 93,01% são utilizadas chaves RSA de 256 bits, recomendadas pelo NIST. Por outro lado, 5,89% dos sites ainda utilizam algoritmos de assinatura obsoletos, como MD5 e SHA1. Dos sites analisados, 204 não obtiveram resultados para algoritmos de assinatura, sendo descartados.

6 Considerações Finais

Realizamos uma análise de 40.406 sites com o objetivo de diagnosticar a saúde do ecossistema HTTPS do Brasil. As descobertas indicam que mais de 98% dos sites ainda suporta versões inferiores a 1.3 do TLS, o que pode colocar em risco os usuários que acessam esses sites. Além disso, apenas 11,01% dos sites suporta a versão 1.3 do TLS, que desde 2018 é reconhecida como a única sem vulnerabilidades identificadas e imune aos ataques conhecidos (e.g., DROWN, PODDLE e BEAST) entre as versões do TLS. Outro fator a ser observado é o grande número de sites utilizando certificados expirados, deixando dados desprotegidos e abrindo brechas para atacantes.

Os resultados indicam a necessidade de avanços quanto ao suporte de diferentes versões do TLS em sites HTTPS no Brasil. Apesar de a maioria dos navegadores já suportarem o TLS 1.3 há algum tempo, a maioria absoluta dos sites HTTPS ainda não suporta essa versão do protocolo. É imprescindível também ter e manter atualizados os certificados TLS, não somente para a segurança das informações, mas também para uma boa reputação do site.

Limitações. A varredura dos IPs incorreu em diversos bloqueios por parte dos provedores de Internet. Uma das formas de mitigar esse problema é implementar algum grau de aleatoriedade na distribuição da carga de trabalho das faixas de endereços IPs (de forma a desagrupar sequências de endereços IPs de um mesmo provedor, por exemplo). Complementarmente, pode-se utilizar ferramentas que permitam uma varredura menos intrusiva e mais difícil de ser detectada, como o `nmap`[1] (<https://nmap.org>).

Trabalhos futuros: (a) aumentar a quantidade de sites analisados; (b) classificar os sites de acordo com setores da economia, buscando identificar eventuais peculiaridades de setores específicos; (c) notificar os sites sobre as vulnerabilidades encontradas; e (d) iniciar campanhas de boas práticas na utilização de HTTPS nos sites.

[1] Ferramentas como o `nmap` permitem definir padrões de temporização (e.g., `-T1 sneaky`) que dificultam o trabalho dos sistemas de detecção.

Referências

EDUCATION, I. C. **Web Server vs. Application Server**. 2020. <https://www.ibm.com/cloud/learn/web-server-vs-application-server?mhsrc=ibmsearch_a&mhq=web%20server>. Citado na página 12.

FIORENZA, M. et al. Uma análise da utilização de https no brasil. In: **Anais do XXXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**. Porto Alegre, RS, Brasil: SBC, 2020. p. 966–979. ISSN 2177-9384. Disponível em: <https://sol.sbc.org.br/index.php/sbrc/article/view/12338>. Citado 5 vezes nas páginas 10, 13, 17, 18 e 21.

Fu, P. et al. Ssl/tls security exploration through x.509 certificate's life cycle measurement. In: **2018 IEEE Symposium on Computers and Communications (ISCC)**. [S.l.: s.n.], 2018. p. 00652–00655. Citado na página 12.

HUANG, J. et al. Assessment of the impacts of tls vulnerabilities in the https ecosystem of china. **Procedia computer science**, Elsevier, v. 147, p. 512–518, 2019. Citado na página 10.

KAPPENBERGER, R. The true cost of self-signed ssl certificates. **Computer Fraud & Security**, v. 2012, n. 9, p. 14–16, 2012. ISSN 1361-3723. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1361372312700921>. Citado na página 12.

VOJTKO, M. **Perfect Forward Secrecy Explained**. 2020. <https://www.thesslstore.com/blog/perfect-forward-secrecy-explained/>. Citado na página 21.

VRATONJIC, N. et al. The inconvenient truth about web certificates. In: **Economics of information security and privacy iii**. [S.l.]: Springer, 2013. p. 79–117. Citado na página 10.