Diagnóstico do Estado de Adopção de Normas de Segurança na Internet Portuguesa

Capítulo Português
da
Internet Society
secretariado@isoc.pt
30/04/2021
Versão 1.0

Internet Society Portugal Chapter
Internet Society Portugal Chapter Foundation

Sumário Executivo

Este documento apresenta um relatório preliminar do Projecto ODIS - sobre a introdução do Capítulo Português da Internet Society (ISOC) - sobre o estado de adopção de normas de segurança e promoção da segurança e da resiliência do sistema de nome e endereços de Internet. Este relatório, que pretende ser o ponto de partida para um processo de diálogo e colaboração entre as diversas entidades interessadas, foi elaborado com base em informação recolhida de fontes abertas e de ferramentas de medição e análise de dados. Os dados e as fontes de informação utilizadas são, nomeadamente, os relatórios do Observatório Sociedade Portuguesa de Inovação, os relatórios do Observatório da Sociedade em Rede da Fundação para a Ciência e a Tecnologia, os relatórios do Observatório das Telecomunicações da Autoridade Nacional das Comunicações, os relatórios do Observatório da Sociedade da Informação do Instituto Nacional de Estatística, os relatórios do Observatório da Sociedade da Informação do Instituto Nacional de Investigação Científica

PARÂMETRO	DESCRIÇÃO
Classificação	Valor da classificação final atribuída ao equipamento de teste internet.nl
Tam IPv6	Os servidores DNS e os servidores SMTP do domínio são acessíveis por IPv6.
Tam DNSSEC	Os filtros correspondentes aos nomes dos servidores estão assinados de forma verificável por DNSSEC.
Tam DNAME	Os servidores DNS aceitam DNAME não-DNSSEC
Tam DKIM	Existe uma entrada DKIM válida no domínio
Tam SPF	Existe uma entrada SPF válida no domínio
Tam STARTTLS	Os servidores de domínio oferecem STARTTLS
Tam versões TLS	O servidor web usa versões TLS/SSL recomendadas.
Tam versões TLS não recomendadas	O servidor web usa versões TLS/SSL recomendadas e não-preferidas.
Tam cipher suites ok	O servidor web usa suites criptográficas adequadas
Tam cipher suites não recomendadas	O servidor usa suites criptográficas adequadas e outras preferidas
Certificado	Os servidores apresentam um certificado X.509 válido colocado e ainda não expirado e a cuja trust chain também foi colocada.
Tam SOAP	Existem entradas DNSSEC válidas no domínio

3. Listas de domínios analisados

Em estudos anteriores, foram analisados os domínios de governo de todos os estados brasileiros, que são: Amazonas, Ceará, Distrito Federal, Espírito Santo, Goiás, Maranhão, Mato Grosso, Mato Grosso do Sul, Minas Gerais, Pará, Paraíba, Paraná, Pernambuco, Piauí, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul, Rondônia, Roraima, Santa Catarina, São Paulo, Sergipe e Tocantins. Também foram analisados os domínios do governo federal, do governo do Estado de São Paulo e do governo do Estado do Ceará. Para o presente estudo, foram analisados os domínios de governo de todos os estados brasileiros, do governo federal e do governo do Estado de São Paulo.

O artigo de Victor e de Freitas et al. [1] que utiliza a base de dados de governo mantida pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br) e que contém a lista de todos os domínios de governo ativos no Brasil, foi utilizado como referência para a coleta dos domínios a serem analisados.

- Lista: https://www.ponto.br/estatisticas/ns-br-0406.txt, acessado em 2 de abril de 2021.

Chaves Criptografadas:

- Lista: https://www.ponto.br/estatisticas/ds-br-0406.txt, acessado em 2 de abril de 2021.

Neste trabalho avaliamos apenas os domínios ativos, conforme a base de dados do NIC.br.

3.1 Lista web hosters

A primeira lista usada neste estudo é a de um conjunto de sites de apoio à modelagem de presença na web para empresários e pessoas físicas. Essas empresas oferecem serviços de hosting, ou seja, contratação de mão-de-obra empresas são desenvolvidas por cliaí sites que oferecem serviços de hosting e que possuem ainda domínios nacionais que são usados em cliaí sites. Essas empresas oferecem serviços de hosting e de mão-de-obra para empresas e não são nacionais, sendo, portanto, não-representativas de uma amostra do universo de sites brasileiros. Foram, ao todo, 17 sites de hosting analisados.

A lista Alexa Top 100 – Portugal corresponde aos 100 sites mais acessados por um usuário da Alexa por Portugal. Os domínios pela Alexa no mês de abril de 2021 foram: Google.com.br, Google.com, Youtube.com, Facebook.com, Instagram.com, Twitter.com, Linkedin.com, Pinterest.com, Netflix.com, Twitch.tv, Mercadolivre.com.br, Amazon.com.br, Amazon.com, Microsoftonline.com, Microsoft.com, Live.com, Office.com, Bing.com, Yahoo.com, Globo.com, Uol.com.br, Mercadolivre.com, Ebay.com, Ebay.com.br, Yahoo.com.br

Tabela 6.2: Caracterização agregada da segurança de serviços de correio electrónico dos domínios que suportam HTTPS, ordenados por ordem decrescente do Alexa 2021, e cruzada com os dados do Tranco 2021 e do Cisco Umbrella 2021 (dados do Alexa Top 500, Significância de primeira coluna explicada na Tabela 2.1)

Lista	Nº total	Nº Alexa
Classificação	33	34
Top Alexa	34%	34%
Tam DNSSEC	1%	1%
Tam DNSSEC	10%	9%
Tam DKIM	23%	10%
Tam SPF	29%	12%
Inclui STARTTLS	28%	16%
Só tem versões TLS recomendadas	25%	12%
Tem versões TLS não recomendadas	25%	42%
Só tem suíte(s) não recomendada(s)	24%	48%
Tem suíte(s) não recomendada(s)	51%	67%
Certificado	19%	67%
Tam Cipher	1%	0%
HTTP headers	0%	1%

7. Contribuição dos ISP

Nesta secção são apresentados os resultados do levantamento de conectividade IPv6, assim como a grau de upstreams e adoção das funcionalidades de conectividade Internet participantes e um conjunto de normas de boas práticas para ISPs. Os resultados do levantamento foram submetidos ao Grupo de Trabalho Técnico da Associação Portuguesa de Operadores de Telecomunicações (APAMT).

Os dados que se seguem foram obtidos através dos observatórios dos APAMT, Labs (https://labs.apamt.pt) e RIPE Atlas. Os dados do RIPE Atlas foram obtidos através da ferramenta usada para realizar as medições, e testar deste consultar a disponibilidade explícita fornecida para APAMT, Labs no seu blog, com exceção dos dados para o ponto de medição a ser discutido.

Muitos dos dados apresentados nesta secção são originados por Sistemas Autónomos no Arquipélago dos Açores, pelo facto de o ponto de medição RIPE Atlas ter sido colocado na rede de um operador de comunicações no ano de Internet (ver ano RIPE). Em Portugal Continental, o ponto de medição RIPE Atlas, um só, só uma rede contribuinte da Internet, com capacidade de participar em decisões de encaminhamento. Nos Açores, o ponto de medição RIPE Atlas está ligado a uma rede contribuinte, mas, perante a Tabela 7.1, é possível observar que existem pelo menos dois diferentes ISPs de Portugal de acordo com o método de medição usado para APAMT, Labs. Como já referenciamos esta não é uma tendência de Portugal Continental, mas, sim, uma tendência de ISPs de Portugal Continental, que, por sua vez, não são contribuintes para RIPE Atlas.

Ao contrário, importante tomar em consideração que o método de observação usado para APAMT, Labs, depende de sondas de ISPs que, por sua vez, são, maioritariamente, ligadas a redes contribuintes Sagres (Internet) e RIPE Atlas. Ou seja, não, pelo menos, ligadas a redes de operadores residenciais pode ser representado nas medidas de forma enviesada. Por isso não são tempo totais o número de unidades de medição para obter um indicador.

A Tabela 7.2 apresenta uma estimativa do grau de perdas entre os utilizadores dos observatórios APAMT, Labs e os operadores de Internet. Nesta tabela, a coluna "Adoção" é o grau de adoção de IPv6 para utilizadores conectados a operadores de Internet que participam no observatório APAMT, Labs. Observe-se que essa disponibilidade apenas é referente entre os utilizadores de 2 dos operadores de Internet que participam no observatório APAMT, Labs. Os restantes operadores de Internet não têm, de momento, sondas IPv6 ou, mesmo, sondas IPv6 ativas. Por isso, a coluna "Adoção" é, de momento, referente a 2 operadores de Internet. Os restantes operadores de Internet, por sua vez, são, maioritariamente, ou, exclusivamente, ligados a redes contribuintes Sagres (Internet) e RIPE Atlas. Observe-se que essa disponibilidade apenas é referente entre os utilizadores de 2 dos operadores de Internet que participam no observatório APAMT, Labs. Os restantes operadores de Internet não têm, de momento, sondas IPv6 ou, mesmo, sondas IPv6 ativas. Por isso, a coluna "Adoção" é, de momento, referente a 2 operadores de Internet. Por sua vez, os restantes operadores de Internet, por sua vez, são, maioritariamente, ou, exclusivamente, ligados a redes contribuintes Sagres (Internet) e RIPE Atlas. Ou seja, pelo menos, ligadas a redes de operadores residenciais pode ser representado nas medidas de forma enviesada. Por isso não são tempo totais o número de unidades de medição para obter um indicador.

Tabela 7.1: Domínios ativos de ISPs de rede ou com em Portugal - dados do observatório APAMT, Labs, obtidos no início de Abril de 2021

ASN	Nº de Sondas	% Nº Sondas	% Nº Sondas
1	42280	NOS Comunicações	1.814.687	60,63%
2	42024	MEO-RESIDENCIAL	2.507.314	31,20	767.666
3	202053	Vodafone Portugal	1.867.533	23,24	571.779
4	202409	MEO-MOVEL	339.821	23,02	566.264
5	43556	ESTEVE Palmela	277.185	2,70	66.499
6	42947	NOS-WINEN	129.694	1,61	39.758
7	42863	NOS-MOVEL	97.034	1,21	29.742
8	204260	CABOVIA	50.879	0,70	17.164
9	42333	VODAFONE	19.763	0,24	5.963
10	43910	RCN NTT, LP	6.642	0,08	2.034
11	43996	CM Lisboa, Portugal	3.906	0,05	1.196
12	42863	MEO-MOVEL	3.498	0,04	1.071
13	42284	NW	3.114	0,04	931
14	204708	LAZER	2.194	0,03	672
15	42333	ALHOLDNOTEC	2.047	0,02	626
16	42333	CLOUDFLARENET	1.752	0,02	537
17	43824	ON-SIP	1.42	0,02	435
18	42333	BLU-AS	1.215	0,02	369
19	42910	UTI-AS	1.146	0,01	351
20	42333	PORTUGALNL-AS	1.122	0,01	344
21	43600	COLT	1.028	0,01	311
22	43487	NG-PT-AS	1.012	0,01	310
23	42333	ZAPNET	947	0,01	290
24	43476	NETSOLUTIONS	921	0,01	281
25	43206	AR TELECOM PT	734	0,01	226
26	42333	ZONE-NATCAL	663	0,01	203
27	42333	TAP-SG TAP-AS PT	361	0,01	172
28	42333	ESP-AS	319	0,00	155
29	42333	NETSOLUTIONS-AS	316	0,00	154
30	42333	NOS-INTERNATIONAL-BCN	426	0,00	130

Tabela 7.2: Utilização de IPv6 em Portugal - dados do observatórios APAMT, Labs, obtidos no início de Abril 2021

ASN	Nº de Sondas	% Nº Sondas	% Nº Sondas
1	42280	NOS Comunicações	0,06%	0,06%	1,39%
2	202053	Vodafone Portugal	13,98%	13,70%	1,81%
3	42024	MEO-RESIDENCIAL	44,0%	42,77%	1,47%
4	202409	MEO-MOVEL	0,80%	0,40%	7,14
5	43556	ESTEVE Palmela	0%	0%	3,93
6	42947	NOS_WINEN	0%	0%	2,34
7	204260	CABOVIA	0%	0%	1,37
8	42863	NOS-MOVEL	0%	0%	1,21
9	204708	LAZER	0%	0%	0,13
10	202053	HOSTROYALE	0%	0%	0,11
11	42333	VODAFONE	0%	0%	0,11
12	43910	RCN NTT, LP	0%	0%	0,1
13	43996	CM Lisboa, Portugal	0%	0%	0,1
14	42333	LAZER	0%	0%	0,1
15	202053	HOSTROYALE	0%	0%	0,1
16	202623	EDP-AS	0%	0%	0,1
17	202623	TEDNET	0%	0%	0,1
18	43600	COLT	0%	0%	0,1
19	204774	MONTES ENG PSC	0%	0%	0,1

Os APAMT, Labs disponibilizam os resultados de seu observatório DNS (APAMT, Resolver) e participam em grupos RIPE Atlas a partir de computadores ligados aos ISPs de Portugal que, por sua vez, que o domínio consultado suporte DNSSEC, e recebeu do consulta foi validado pelo resolver utilizado. Ou seja, o domínio que o resolver tem de validar a assinatura DNSSEC e que o domínio que o resolver tem de validar a assinatura DNSSEC e que o domínio que o resolver tem de validar a assinatura DNSSEC e que

de segurança pelos servidores de correio HTTPS; (2) a análise do grau de penetração de normas de segurança nos servidores de correio electrónico (servidores SMTP) das instituições observadas; (3) na análise da contribuição para a segurança da Internet portuguesa de algumas empresas relevantes que actuam em Portugal como fornecedores de serviços de web hosting, e (4) na análise da contribuição dos ISPs portugueses para a disseminação de suporte IPv6, das normas DNSSEC e das normas associadas às boas práticas de encaminhamento seguro, nomeadamente, o progresso da adesão à norma MANRS e RPKI. O diagnóstico resultante e o referencial suportado pela plataforma de software do observatório OSSE permite uma análise criteriosa/objectiva/detalhada do estado da segurança da adopção das normas e melhores práticas de segurança centrada a uma Internet mais segura e confiável para todos os utilizadores. A partir do diagnóstico e observações de detalhe, o observatório OSSE permite formular um conjunto de recomendações que teriam um impacto decisivo na melhoria das métricas e práticas de segurança observadas.

Os resultados e observações apresentadas no relatório privilegiam a apresentação de resultados agregados. Não obstante, as observações realizadas permitiram obter observações agregadas por sector, permitindo análises comparativas entre os diferentes sectores. Isso poderia ajudar a progressos sectoriais, dado que permitiria destacar esforços sectoriais, que de outra forma ficariam diluídos no conjunto.

Segue-se a exposição das conclusões gerais resultantes da actual observação OSSE que decorrem dos resultados apresentados no relatório completo.

9.1 Servidores HTTPS e sua parametrização

É possível, e necessário, melhorar significativamente a base de segurança da utilização da Internet e da exposição web em Portugal. Isso evitaria que várias organizações exponham "uma imagem menos interessante" ou apresentem "uma presença deficiente e mais vulnerável".

Dificilmente se encontram entidades que consigam atingir classificações superiores a 80 na escala usada, que vai de 0 a 100. A maioria das entidades observadas ficam classificadas de forma intermédia (próximo de 50) nessa escala. Por outro lado verifica-se que existem algumas instituições e sectores com fragilidades muito acentuadas, seja porque eviteem grande vulnerabilidade no suporte HTTPS, ou porque nem sequer adoptam HTTPS.

Nesta vertente, as seguintes acções parecem ser necessárias.

1. Promoção de uma gestão com um controlo mais fino e mais rigoroso dos parâmetros de segurança TLS e da criptografia "ponta-a-ponto" que lhe está subjacente. Em particular a abandono imediato das versões deprecated de TLS, ou seja, abandono de TLS1.0 e TLS1.1 (11) e transição de TLS1.2 para TLS1.3.

2. O reforço da utilização dos headers de segurança HTTP e do suporte DANE, em articulação com adopção de DNSSEC.

3. Particular atenção deve prestada à inclusão do suporte de HSTS e de OCSP Stappling.

Estas acções permitiriam obter uma base mais sólida para a segurança dos serviços e aplicações web, com melhores defesas e mitigação das vulnerabilidades passíveis de serem articuladas com outros vectores de ataques à web portuguesa, bem como corrigir, a curto prazo, as deficiências muito gritantes que se verificam em alguns sectores.

9.2 Servidores de correio electrónico e sua parametrização

A observação do estado da segurança do ecossistema de correio electrónico em Portugal revela resultados bastante deficientes e necessitadas de correcções significativas. Na maior parte das entidades observadas, as classificações, novamente numa escala de 0 a 100, são tranformente insuficientes (em geral abaixo de 50 e em grande parte abaixo de 30). Embora o trabalho futuro a ser desenvolvido no observatório deva abarcar uma análise progressivamente mais fina de todo este ecossistema, algumas conclusões resultam imediatamente da observação realizada, nomeadamente:

1. A reduzida penetração DNSSEC nos domínios associados aos endereços do correio. Tal tem um impacto significativo na segurança da informação anti phishing registada nos domínios DNS relevantes.

2. A não conformidade ou a incompletude do suporte ao correio electrónico seguro, nomeadamente a introdução no DNS dos registos: DKIM, DMARC e SPF, e a necessidade da introdução de transporte seguro do correio através do suporte de STARTTLS nos servidores SMTP.

Estando o eco-sistema de correio electrónico particularmente associado a vectores de ataque com grande relevância actual, o reforço das práticas de segurança listadas acima e a adopção das respectivas normas, não constituindo por si só a panacea para a globalidade desses ataques, poderia, no entanto, constituir uma importante base comum de incremento de garantias de segurança, associadas a outras, necessárias, medidas complementares.

9.3 Empresas de web hosting

Os chamados web hosters podem contribuir de forma muito significativa para o aumento da segurança da Internet portuguesa dado o impacto que as normas que adoptam têm em todo o tecido dos seus clientes, constituído essencialmente por empresas de pequena ou média dimensão.

Estes prestadores de serviços devem consolidar uma rede de segurança capaz de evitar a adoção dos serviços que prestam a partir de operadores internacionais, o que pode ser um aspecto relevante na responsabilidade e base de jurisdição desse tipo de suporte, equilibrando a desintermediação no sector e as consequentes dificuldades que por vezes daí decorrem. Este aspecto poderá ser particularmente relevante de acautelar na estratégia de hosting de serviços públicos ou de entidades do Estado, incluindo as questões que decorrem da certificação digital XS09 não intermediada ou gerida em Portugal.

Dado o impacto destes prestadores de serviços na transição digital de muitas organizações, e na promoção de uma economia digital, este sector poderá justificar uma intervenção específica.

As observações realizadas mostram que alguns destes prestadores de serviços já fizeram um trabalho que se reflete em propriedades de segurança mais elevadas da sua oferta de serviços. Outros, no entanto, apresentam limitações na sua oferta que deveriam ser ultrapassadas. E importante caminhar-se para um maior comprometimento e valorização dos fornecedores com uma oferta de soluções mais seguras, através das seguintes ações:

1. Abandono imediato de TLS 1.0 e TLS 1.1 e de Secure Socket Layer (SSL) e fomento da migração gradual de TLS 1.2 para TLS 1.3, logo que possível.

2. Reforço do suporte de HSTS e de OCSP Stappling e melhoria do suporte dos headers HTTP de segurança.

3. Imediata disponibilidade de DNSSEC e suporte de DANE e disponibilidade progressiva de IPv6.

4. Melhoria significativa do serviço de correio electrónico oferecido, nomeadamente através da introdução no DNS dos registos: DKIM, DMARC e SPF, e a necessidade da introdução de transporte seguro do correio através do suporte de STARTTLS nos servidores SMTP.

9.4 ISPs portugueses

Os ISPs deverão continuar a reforçar a oferta de resolvers com suporte de DNSSEC e adoptarem de forma vigorosa o conjunto de boas práticas de encaminhamento recomendadas pela iniciativa MANRS (mans.org). Neste campo a situação parece ser caracterizada por um progressivo alastramento do registo de ROAs, mas uma adopção tímida de filtragem com base na infraestrutura RPKI.

Infelizmente, ao que parece, ainda nenhum ISP comercial português adoptou a prática de exibir o selo de qualidade MANRS, dado o não comprometimento oficial com a iniciativa.

Finalmente, os esforços para disponibilizar endereçamento e conectividade IPv6 necessitam de uma adesão mais vigorosa dos ISPs que já o fazem, e de que os restantes se decidam a avançar com essa oferta.

9.5 Sobre a visibilidade, reconhecimento e compromisso com a segurança da Internet em Portugal

E necessário promover uma maior visibilidade e reconhecimento pelas empresas prestadoras de serviços de web hosting e pelos ISPs das características de segurança dos serviços que providenciam, e é também necessário levar a que os clientes valorizem esses esforços, descartando os fornecedores que os ignorem, de modo a que os esforços de incremento da base de segurança da Internet em Portugal sejam recompensados.

Esta frente, que tem sido acautelada em muitos países através da colaboração de diferentes entidades, com diferentes papéis, exige uma abordagem colaborativa. Este parece continuar a ser um terreno que precisa de ser percorrido com mais entusiasmo, envolvimento e comprometimento, para lá das iniciativas localizadas, por vezes orientada para resultados mais limitados no alcance e na efectividade.

A nossa esperança e desejo é que o observatório OSSE contribua, ainda que modestamente, e mais pelo exemplo, para que se caminhe para a criação de condições de valorização de uma "economia da segurança" e, consequentemente, de uma maior exigência por parte dos consumidores. A divulgação de métricas de comprimento/cumprimento por parte de entidades prestadoras de serviços para a melhoria da situação actual, o reconhecimento da diferenciação da qualidade da oferta de serviços por

parte dos players envolvidos, o estabelecimento de quadros de colaboração e parceria "multi-stakeholder" para o reforço das práticas de segurança e o aumento progressivo da exigência dos consumidores, são outras tantas vias para a promoção do nível de segurança da Internet portuguesa.

As entidades de regulação e o sector público podem desempenhar um importante papel através de uma intervenção, primeiro pedagógica, e depois de carácter regulatório. O usufruto das vantagens da transição digital só pode ter lugar num quadro de garantias de segurança a todos os níveis para os utilizadores e empresas. Caso

contrário, não é expectável senão um incremento dos inevitáveis problemas que essa transição acarreta, e um decréscimo significativo das vantagens que potencia.

Bibliografia

[1] R. Fielding (Ed.) and J. Reschke (Ed.), "Hypertext Transfer Protocol (HTTP/1): Message Syntax and Routing." RFC 7230 (Proposed Standard), June 2014. Updated by RFC 8615.

[2] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3." RFC 8446 (Proposed Standard), Aug. 2018.

[3] J. Klensin, "Simple Mail Transfer Protocol." RFC 5321 (Draft Standard), Oct. 2008. Updated by RFC 7504.

[4] D. Margolis, M. Risher, B. Ramakrishnan, A. Brotman, and J. Jones, "SMTP MTA Strict Transport Security (MTA-STS)." RFC 8461 (Proposed Standard), Sept. 2018.

[5] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification." RFC 8200 (Internet Standard), July 2017.

[6] P. Hoffman, A. Sullivan, and K. Fujiwara, "DNS Terminology." RFC 8499 (Best Current Practice), Jan. 2019.

[7] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS Security Introduction and Requirements." RFC 4033 (Proposed Standard), Mar. 2005. Updated by RFCs 6014, 6840.

[8] G. Huston, G. Michaelson, C. Martinez, T. Bruijnzeels, A. Newton, and D. Shaw, "Resource Public Key Infrastructure (RPKI) Validation Reconsidered." RFC 8360 (Proposed Standard), Apr. 2018.

[9] R. Bush, R. Volk, and J. Heitz, "Resource Public Key Infrastructure (RPKI) Origin Validation for BGP Export." RFC 8893 (Proposed Standard), Sept. 2020.

[10] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." RFC 5280 (Proposed Standard), May 2008. Updated by RFCs 6818, 8398, 8399.

[11] K. Moriarty and S. Farrell, "Deprecating TLS 1.0 and TLS 1.1." RFC 8996 (Best Current Practice), Mar. 2021.

[12] V. L. Pochat, T. Van Goethem, S. Tajalizadehkhoob, M. Korczyński, and W. Joosen, "Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation," Proceedings 2019 Network and Distributed System Security Symposium, 2019. arXiv: 1806.01156.

[13] T. Bates, R. Chandra, D. Katz, and Y. Rekhter, "Multiprotocol Extensions for BGP-4." RFC 2283 (Proposed Standard), Feb. 1998. Obsoleted by RFC 2858.

[14] Y. Rekhter (Ed.), T. Li (Ed.), and S. Hares (Ed.), "A Border Gateway Protocol 4 (BGP-4)." RFC 4271 (Draft Standard), Jan. 2006. Updated by RFCs 6286, 6608, 6793, 7606, 7607, 7705, 8212, 8654.

[15] S. Weiler (Ed.) and D. Blacka (Ed.), "Clarifications and Implementation Notes for DNS Security (DNSSEC)." RFC 6840 (Proposed Standard), Feb. 2013. Updated by RFC 8749.

[16] R. Mohapatra, J. Scudder, D. Ward, R. Bush, and R. Austein, "BGP Prefix Origin Validation." RFC 6811 (Proposed Standard), Jan. 2013. Updated by RFCs 8481, 8893.

[17] R. Bush, "Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)." RFC 7115 (Best Current Practice), Jan. 2014.

Siglas Usadas

APNIC Asia Pacific Network Information Centre

AS Autonomous System

BGP Border Gateway Protócol

ccTLD country code Top-Level Domain

CNCS Centro Nacional de Ciber Segurança de Portugal

DANE DNS-Based Authentication of Named Entities

DNS Domain Name Service

DNSSEC Domain Name System Security Extensions DKIM DomainKeys Identified Mail

DMARC Domain-based Message Authentication, Reporting and Conformance

HSTS HTTP Strict Transport Security

HTTP Hyper Text Transfer Protocol

HTTPS Hyper Text Transfer Protocol Secure IETF Internet Engineering Task Force IPv4 Internet Protocol Version 4

IPv6 Internet Protocol Version 6

IRR Internet Regional Registry

ISOC Internet Society ISOC PT Capítulo Português da Internet Society ISP Internet Service Provider

MANRS Mutually Agreed Norms for Routing Security

OCSP Online Certificate Status Protocol

OSE Open Standards Everywhere

OSSE Open Security Standards Everywhere

ROA BGP Route Origination Authorization

RPKI Resource Public Key Infrastructure

SMTP Simple Mail Transfer Protocol

STARTTLS SMTP will be executed over TLS/SSL

SSL Secure Socket Layer

SPF Sender Policy Framework

TLS Transport Layer Security

Capítulo Português da Internet Society

osse@isoc.pt