ICANN 60
ANNUAL GENERAL

ABU DHABI

28 October–3 November 2017

RELATÓRIO DNS.PT

ÍNDICE

INTRODUÇÃO

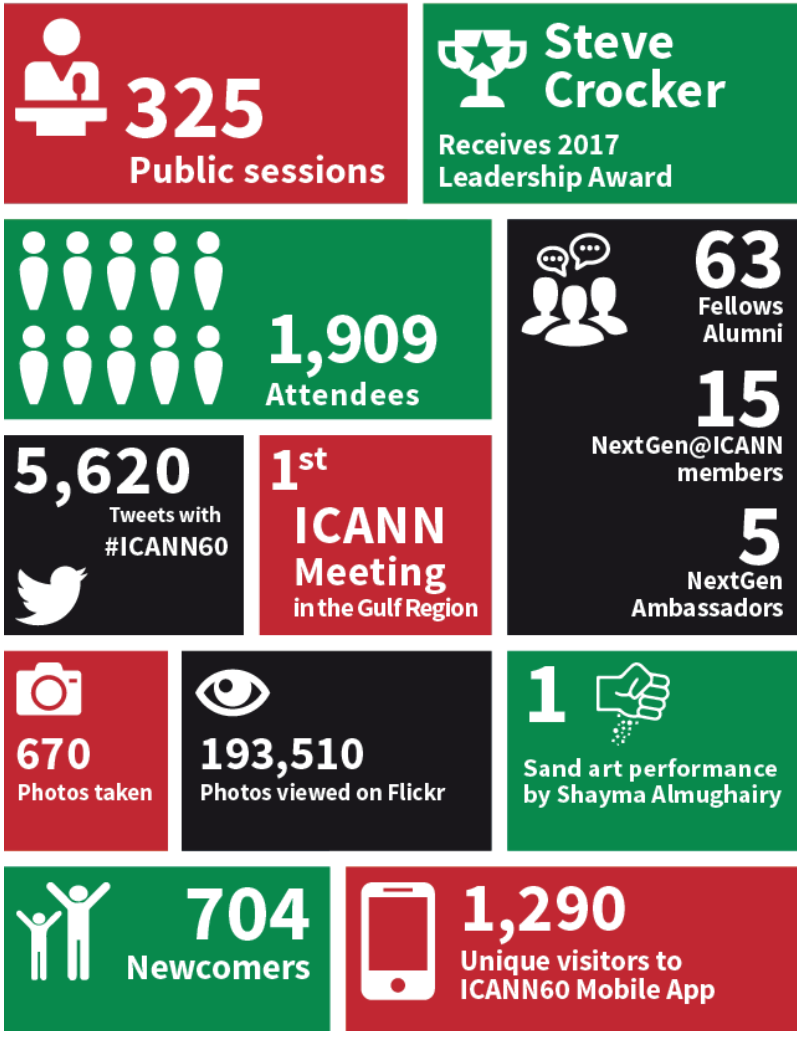
A ICANN 60 decorreu entre os dias 28 de outubro e 3 de novembro, na capital dos Emirados Árabes Unidos, Abu Dahbi, sob o olhar atento de uma comunidade que, *ex ante*, manifestou alguma desconfiança relativamente aos padrões culturais e sociais a que se teria de adaptar ao longo dos 7 dias de reunião. Não houve percalços conhecidos, e tudo decorreu conforme o planeado.

Steve Crocker, autor do primeiro RFC datado do já longínquo ano de 1969, reconhecido como um dos pioneiros da internet, despede-se nesta edição de chair do board, cargo que já ocupava desde junho de 2011. O egípcio Cherine Chalaby passa agora a liderar o board da ICANN ao lado do australiano Chris Disspain, ex chair do ccNSO, e que agora assume a vice-presidência.

Nesta edição, para além das relevantes matérias de natureza técnica, com especial destaque para a suspensão do KSK Rollover[1], o assunto mais debatido foi sem dúvida o impacto do Regulamento Geral de Proteção de Dados na continuidade do WHOIS como hoje o conhecemos. Na mesa, e a este propósito, ficou a questão: *What happens if WHOIS goes dark*?

1 *https://www.icann.org/news/announcement-2017-09-27-pt*

ICANN 60 EM NÚMEROS



Em repetição esteve o tópico da utilização dos nomes de países e territórios como domínios de topo. Esta questão tem especial acuidade no caso da ICANN vir a abrir um novo processo de candidaturas para nGTL's, o que não se perspetiva acontecer antes de 2019.

Esta mesma questão foi discutida na Assembleia Geral do CENTR no passado mês de outubro, na sequência das conclusões apresentadas pelo *Work Track 5* da *ICANN* (*Cross Community Working Group on the Use of Country and Territory Names as TLDs*) que, na prática, não apresentou soluções, vindo apenas ao fim de três anos de trabalho apontar questões para um problema que já se vem antecipando e onde ainda não há consenso. Entretanto o CENTR veio já apresentar a sua posição formal nos termos da qual:

- Todos os Códigos ASCII de 2 letras, estejam ou não na lista ISO-3166-1 alfa-2, são reservados para uso exclusivo como ccTLDs presentes e futuros;
- Os códigos ASCII de 3 letras na lista de alfa-3 ISO 3166-1 devem permanecer bloqueados e não registáveis como novos gTLD, o que significa que as restantes mais de 17,576 combinações de 3 letras ficam disponíveis para utilização como novos gTLDs;
- Deverão ser mantidas as restantes restrições fixadas a este propósito no Guia do Candidato de 2012[2].

https://centr.org/library/library/policy-document/centr-position-on-the-use-of-country-and-territory-names-as-tlds.html

[2] *https://newgtlds.icann.org/en/applicants/agb*

Outra questão paralela, mas claramente associada à anterior, é a utilização dos códigos dos países, o .pt, por exemplo, como domínios de segundo nível. Diga-se que cerca de 84% dos registries de ccTLD's de todo o mundo já o permitem sem qualquer nível de restrição[3]. Relativamente aos novos gTLD mantém-se o enquadramento definido pelo Board. Recapitulando, em 1 de Dezembro de 2014 a ICANN autorizou a liberalização dos códigos de países de dois caracteres especificados na ISO 3166/2, no segundo nível nos novos gTLDs, no sentido de promover a concorrência no mercado de nomes de domínio, desde que o governo e o Registry do país interessado fosse notificado para se pronunciar .

O gTLD Registry que pretendesse a utilização dos códigos com dois caracteres de países especificados na norma ISO 3166/2, tinha duas opções, ou interpelava diretamente o governo e a entidade gestora do ccTLD em questão, sobre a sua permissão para a utilização desses códigos ou solicitava essa aprovação diretamente através da ICANN. Na última opção, os governos seriam notificados, ou pelo menos os que o queriam o ser, e tinham 60 dias para oposição. Os interesses de ambas as partes estavam pois tutelados.

O panorama mudou com a resolução do Board tomada em 8 de Novembro de 2016, em Hyderabd, e a sua implementação, em 13 de dezembro de 2016, que permitiu a liberalização de todos os códigos de dois caracteres previamente reservados, facto que terá surpreendido a comunidade. Nesse mesmo sentido algumas vozes discordantes fizeram-se ouvir no GAC e no ccNSO.

Esta autorização geral, materializada no cancelamento do período de resposta de 60 dias, gerou discordância de alguns governos parte do GAC, que tinha dado parecer ao Board no sentido oposto. Embora haja dentro do próprio GAC, países e territórios que defendem a posição do Board, outros defendem que está em causa o interesse público, pelo que salvo se o governo ou o Registry que é responsável pela gestão do código do país tenha prestado o seu consentimento através de uma carta formal, tal não deverá ser permitido. Consequentemente, a ICANN58 foi marcada pela insatisfação do GAC nesta matéria.

O GAC vai mais além, afirmando mesmo que não houve transparência na condução deste processo de liberalização e que a utilização dos códigos de dois caracteres pelos novos gTLD's devem permanecer reservados aos ccTLDs. Mais, na perspetiva do GAC o conjunto de requisitos impostos pela ICANN são muito pouco exigentes, não protegendo os ccTLDs.

3 *Em .pt não são admitidos registos de nomes coincidentes com domínios de topo.*
Trata-se de uma regra espelhada na al. b) do n.º 1 do artigo 9.º do Regulamento de Registo de Domínios de .pt, aprovado em junho de 2014.

Ora, a realidade atual é que vários novos gTLD's já têm registado como domínios de segundo nível códigos de países[4]. Diferente, porém, é o registo do próprio nome do país, o que claramente vai para além de apenas o próprio código ISO. Portugal, inclusivamente, tem sido por diversas contactado no sentido de permitir o registo do nome do país, o que ainda não aconteceu. Entretanto, no decurso desta edição da ICANN, esta questão foi de novo levada a discussão no seio do GAC, onde o representante do governo da Índia, a propósito do enquadramento que hoje está a ser feito pelo gTLD .ECO, defendeu a pertinência da proteção total dos códigos e nomes de países e territórios em sede de registo como domínios de segundo nível junto dos novos gTLD's. Os argumentos aduzidos centram-se nas matérias que alvitram à volta da confundibilidade e concorrência desleal, mas também, em última análise, no facto de com isto se puder estar a, digamos, "arranhar" o princípio da soberania dos países.

4 *Veja-se no caso de .pt: www.pt.abbott; www.pt.asia, etc.*

"WHAT HAPPENS IF WHOIS GOES DARK"

O Regulamento Geral de Proteção de Dados[5](RGPD) e aquilo que são já hoje as implicações do seu articulado no processo associado ao registo de domínios nas suas múltiplas vertentes - seja a montante, com a forma de recolha e tratamento dos dados pessoais de quem regista e gere a vida de um domínio ou depois, a jusante, com os dados pessoais que são divulgados ao mundo, especialmente via WHOIS[6] - foi outro dos assuntos mais debatidos na ICANN ao longo dos sete dias desta última reunião do ano. E a importância do tópico inferiu-se não só pelo número de horas de discussão mas também, e sobretudo, por quem nelas participou. Toda a comunidade esteve envolvida, todos os grupos de trabalho, o board da ICANN, o próprio presidente da ICANN, vários representantes da Comissão Europeia, diferentes Autoridades de Proteção de Dados[7], o que sem dúvida espelha a perceção generalizada do impacto deste novo quadro legal da privacidade e proteção dos dados pessoais, que extravasa as hipotéticas fronteiras dos 28 países da União Europeia.

Esta última nota é fundamental se pensarmos que a ICANN, enquanto instituição sem fins lucrativos, é uma organização sediada no estado da Califórnia, e que, como

5 *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016*

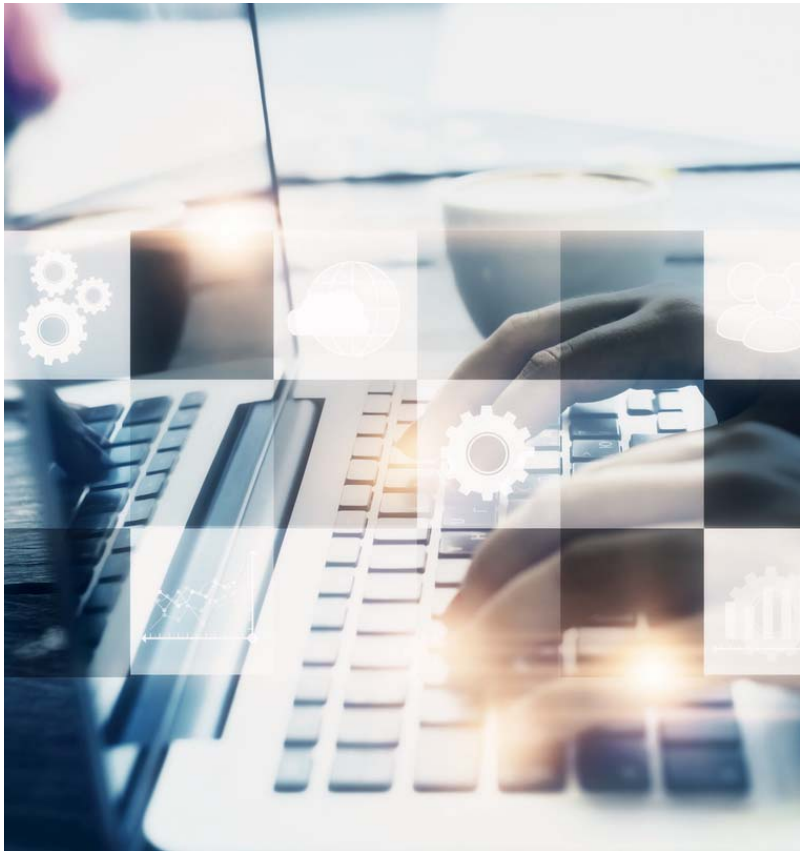
6 *Exemplo de resultados WHOIS para o domínio dns.pt: https://www.dns.pt/pt/ferramentas/whois/detalhes/?site=DNS&tld=.pt*

7 *Foi referido existirem atualmente mais de 120 países em todas as regiões do mundo que incluem no seu ordenamento jurídico leis de privacidade e proteção de dados pessoais.*

tal, se rege na sua essência e naquilo que é o seu funcionamento e forma de interação com registries e registrars de todo o mundo, pelos seus estatutos e pela lei americana[8].

Uma primeira nota a este respeito recaiu sobre o facto do RGPD, sendo relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, assenta na essência nas bases e princípios da sua antecessora Diretiva 95/46/CE[9], do Parlamento e do Conselho, de 24 de outubro de 1995[10]. Ora, com isto é oferecida à ICANN uma nova oportunidade para resolver e cumprir com as regras de privacidade e proteção de dados que também lhe são aplicáveis e, como isso, contribuir para garantir a estabilidade, solidez e precisão do WHOIS. Neste contexto, a Comissão Europeia recomendou expressamente que seja adotada uma abordagem coordenada para garantir o cumprimento das regras de proteção de dados, de forma a preservar, por exemplo, o acesso legítimo às informações WHOIS.

A Comissão Europeia referiu ainda a este propósito que o RGPD sendo exigente disponibiliza uma série de ferramentas em termos de base legítima para o processamento (consentimento, execução de um contrato, interesse legítimo, etc.), e transferências internacionais que devem ser avaliadas e podem ser utilizadas para operar e suportar a utilização legítima de sistemas como o WHOIS. Ou seja, nas palavras de um participante "(...)há soluções e não é uma espécie de Armageddon".



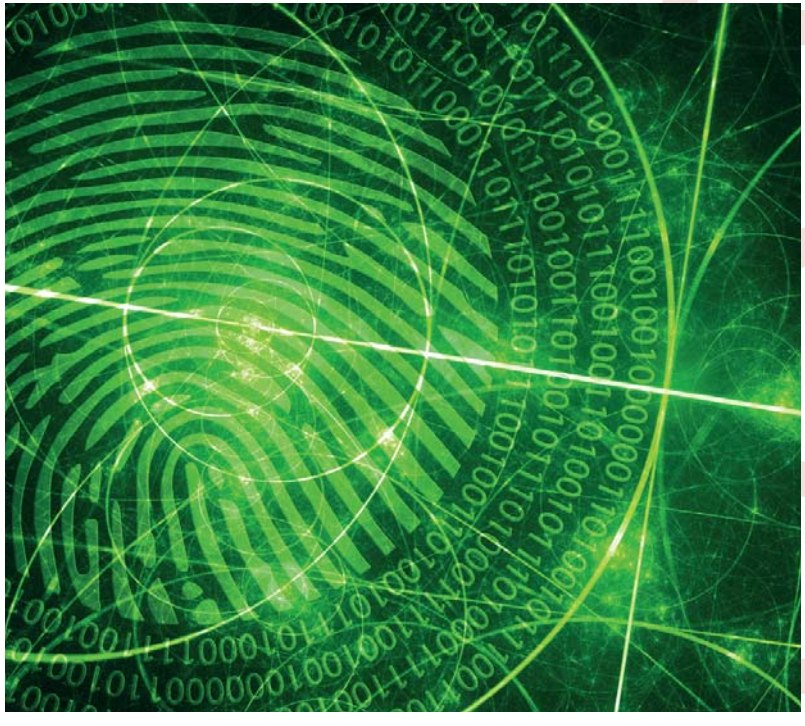
8 *Estatutos ICANN, versão integral disponível em: https://www.icann.org/resources/pages/governance/bylaws-en/#article1. Section 1.2. COMMITMENTS AND CORE VALUES*
In performing its Mission, ICANN will act in a manner that complies with and reflects ICANN's Commitments and respects ICANN's Core Values, each as described below.(a) COMMITMENTS In performing its Mission, ICANN must operate in a manner consistent with these Bylaws for the benefit of the Internet community as a whole, carrying out its activities in conformity with relevant principles of international law and international conventions and applicable local law, through open and transparent processes that enable competition and open entry in Internet-related markets. Specifically, ICANN commits to do the following (each, a "Commitment," and collectively, the "Commitments")

9 *Transposta para o ordenamento jurídico português pela Lei n.º67/98, acessível para consulta em: https://www.cnpd.pt/bin/legis/nacional/lei_6798.htm*

10 *Nota curiosa registada no decurso de uma sessão: RGPD é uma evolução e não uma revolução!*

Ora, o grande problema aqui é claramente o WHOIS, pelo menos o problema mais visível e impactante[11]. Através deste sistema[12] o publico em geral tem acesso a informação mais ou menos completa – já que não há uma estandardização universal do WHOIS – sobre o titular do nome de domínio e os responsáveis pela gestão do mesmo. A título de exemplo a ferramenta de WHOIS disponibilizada em dns.pt disponibiliza, relativamente a cada domínio, os seguintes dados: nome de domínio; data de submissão; data de expiração; estado; identificação do titular (nome, morada e email); identificação dos dados relativos à entidade gestora e ao responsável técnico e, por fim, informação do nameserver. O problema aqui é fácil de identificar: alguns destes dados podem ser qualificados como dados pessoais. Diga-se, indo buscar algo já atrás referido, que nada disto é novo. Olhando agora apenas para o panorama nacional, a nossa Lei de Proteção de Dados dava já tutela jurídica a estes dados e, nessa medida, o .pt estava já vinculado ao cumprimento estrito da mesma, o que de resto hoje já acontece. Nessa medida a recolha de dados é já feita de acordo com o âmbito do consentimento[13] do seu titular e o WHOIS[14] apenas disponibilizada os dados para os quais está autorizado.

A resposta imediata pode ser muito simples: acabe-se com o WHOIS! O problema, ou uma parte muito significativa dele, fica resolvido. Técnica ou contratualmente não haveria aqui qualquer contrariedade para se avançar nesse sentido. Salvo no caso dos gTLD's que têm uma obrigação contratual[15] [16] com a ICANN de disponibilizar o WHOIS com um determinado perfil, os ccTLD's não têm qualquer vínculo com força efetiva nessa mesmo sentido.



11 *O ICANN vai ter outros, veja-se por exemplo, como irá ser tratada a recolha e tratamento dos milhares de dados pessoais que resultam dos processos de inscrição em cada reunião da ICANN.*

12 *Estão já a ser pensadas pela comunidade técnica alternativas mais evoluídas para este sistema, por exemplo o RDAP.*

13 *O consentimento assume contornos no âmbito do RGPD que vão para além daquilo que eram as exigências da ainda vigente Lei de Proteção de Dados. Referimo-nos, no caso vertente, ao cumprimento do previsto nesta Lei.*

14 *Referimo-nos ao WHOIS acessível via dns.pt.*

15 *Veja-se: https://newgtlds.icann.org/en/applicants/agb/agreement-approved-02jul13-en.pdf*

16 *Considere-se, no entanto, as palavras de Göran Marby, que passamos a citar: (...) ICANN contracted compliance will not take action against any registry or registrar for non-compliance with their obligations related to the handling of registration data. If a contracted party intends to deviate from existing obligations it must share its model with ICANN."*

Esta solução, sendo possível, mereceu a critica de muitos, pela seguinte ordem de razões: o WHOIS contribui para a segurança e estabilidade da Internet e, como tal, deve ser visto como um recurso de interesse público, em suma um recurso que também é, e deve continuar a ser, disponibilizado de forma aberta e generalizada aos consumidores em geral. Por outro lado, os resultados gerados pelo WHOIS podem ser determinantes para identificar, por exemplo no âmbito de investigação de crimes, os respetivos autores, ou mesmo avaliar, prevenir e mitigar eventuais ataques que diariamente põem em causa a segurança de redes informáticas criticas.

A réplica a estas criticas foi obviamente imediata, se por um lado muitos dos dados disponibilizados hoje no WHOIS não são confiáveis, na medida em que são literalmente falsos, por outro lado nada impede que os registries continuem a disponibilizar os dados na sequência de pedidos devidamente fundamentados, que não têm forçosamente de ser veiculados apenas por tribunais ou órgãos de polícia criminal. Nesta longa malha, surge logo outro problema: e quando aos registries chegarem centenas de pedidos para processar? Qual o impacto para uma investigação criminal de um pedido de resposta que demora dias a processar? e isto será fácil de antever considerando os milhares[17] de pedidos que diariamente são feitos a nível mundial à base de dados do WHOIS.

Göran Marby, presidente da ICANN, anunciou que a ICANN está fortemente empenhada em encontrar uma solução capaz de ir ao encontro dos interesses de toda a comunidade, e está inclusivamente já hoje trabalhar nisso[18] indo nas próximas semanas anunciar três alternativas a avaliar pelos interessados. Em qualquer dos casos estará à partida posta de parte qualquer solução que ponha fim ao WHOIS.

Göran Marby: "We cannot accept to go away from full WHOIS".

Há que chegar a um equilíbrio entre aquilo que é o interesse público e a necessária tutela de direitos fundamentais de privacidade e proteção de dados pessoais. O exercício já feito pela comunidade de

17 *Reproduzimos aqui as palavras de Pierre Bonis, que partilhou neste âmbito a experiência do .fr "(...) With more than 3 million domain names, there have been 400 requests per year to access WHOIS, which have been dealt with within less than a day – and these were not from IP law firms or law enforcement. "This is maybe not the nightmare that someone fears".*

18 *Nesse sentido: https://www.icann.org/resources/pages/contractual-complance-statement-2017-11-02-en*

identificar porque é que o WHOIS é importante, porque é que esta base de dados tem de existir e estar universalmente visível e acessível, é já um primeiro passo. O passo seguinte, norteados por princípios como a transparência, a qualidade dos dados e a minimização, será o de elencar de forma objetiva que dados associados ao domínio são verdadeiramente necessários para concretizar os fins do WHOIS. Esse é outro desafio.

Segue-se outra tarefa, digamos, não menos inglória, determinada a natureza dos dados que vão ser disponibilizados, avaliar as medidas a tomar para que os mesmos sejam recolhidos e tratados ao abrigo das disposições do RGPD, o que pode, no limite, passar pela criação de mecanismos de anonimização.

O último dos desafios tem uma concretização (ainda mais) difícil, encontrar uma solução uniforme entre as diversas plataformas de WHOIS a que hoje todos nós podemos aceder. Aqui, organizações como a ICANN e, a nível regional, o CENTR, a AFNIC a APTLD, o LACNIC e mesmo a LusNIC, podem ser uma valia.

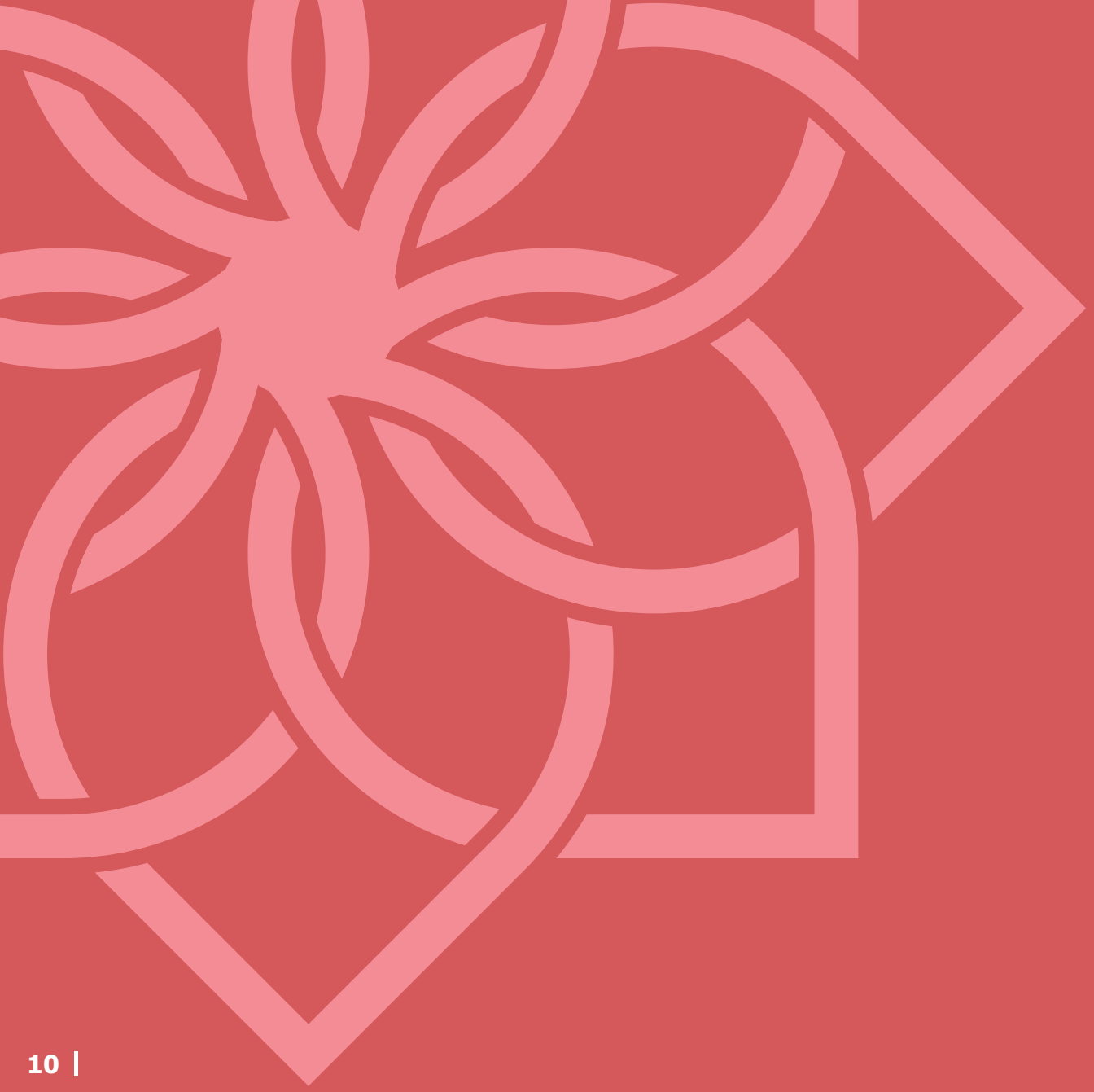
Até lá temos meio ano.

Saiba mais em:

Relatório CENTR: https://centr.org/library/library/external-event/centr-report-on-icann60.html

Comunicado do GAC: https://gac.icann.org/advice/communiques/public/gac-60-abu-dhabi-communique.pdf

ICANN | 60 • TECH DAY



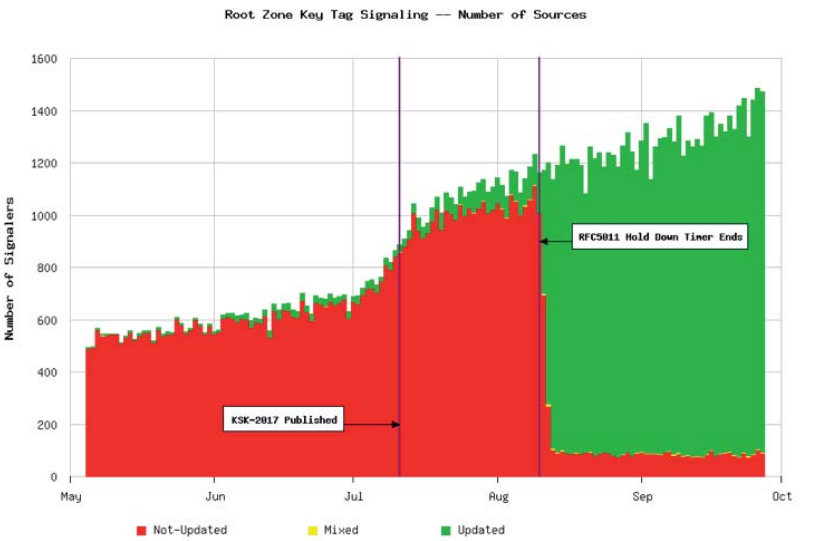
SUSPENSÃO DO PROCESSO KSK ROLLOVER

A suspensão da Root KSK Rollover é um tema em grande destaque, ou não fosse este potencialmente impactante para a segurança e estabilidade da internet e de um número ainda incerto de utilizadores.

Roy Arends, responsável pela área de investigação da ICANN, fez uma breve apresentação sobre os motivos, os dados observados, as dificuldades encontradas e os planos para dar continuidade ao processo de Rollover.

Até recentemente, não era possível consultar a chave Trust Anchor de DNSSEC utilizada em cada servidor resolver, mas o desenvolvimento do mecanismo Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC), RFC 8145, veio dar essa possibilidade. Porém, por se tratar de uma nova solução, este apenas existe nas implementações de software de DNS mais recentes, Bind 9.11.0b3 e 9.10.5b1, e Unbound 1.6.4.

Durante os meses de setembro e outubro, e com recurso a este mecanismo, a ICANN recolheu e analisou o tráfego DNS de 27,084 servidores resolvers com DNSSEC, dos quais 6,02% não reconheceram a nova chave (KSK-2017) quando tal era suposto. Note-se, que a amostra de endereços analisados, representa apenas 0,57% dos 4.2 milhões de endereços possíveis.



Fonte: https://blog.verisign.com/domain-names/root-zone-ksk-rollover-postponed/

Nesta imagem, é visível o momento a 10 de agosto, quando a número de servidores atualizados com a nova chave, representados a verde, deveria ser total. Contudo, um pequeno, mas não desprezível número de sistemas, continuou a reconhecer apenas a chave atual. Esta circunstância está representada por uma pequena lista a vermelho nos meses seguintes.

Perante estes dados, a 27 de setembro, a ICANN suspende[19] temporariamente o processo de Rollover, e inicia uma análise detalhada aos dados encontrados, nomeadamente uma lista de 1.631 servidores, cuja sinalização, não indicava uma configuração de chaves válida.

19 *https://www.icann.org/news/announcement-2017-09-27-en*

A ICANN reconhece que a análise é bastante complexa, sobretudo porque não é possível garantir que o número de sistemas afetados é verdadeiramente real. Há vários motivos para um servidor responder de forma incorreta, nomeadamente erros de implementação e de configurações incorretas no software DNS.

Partindo da lista de 1.631 servidores em falha, a ICANN contratou um consultor externo para entrar em contacto com os responsáveis de 500 deles e para descobrir e corrigir o motivo da falha. Esta tarefa encontra-se na fase inicial da sua execução, tendo sido identificado o motivo da falha em apenas 0,8% dos sistemas. Destes, 8,7% tinham uma configuração manual quando julgavam que tinham uma configuração automática. Pelo RFC 5011, 4,3% estavam configurados com suporte do RFC 5011 mas problemas de permissões de escrita em disco impediam a atualização automática da chave, e a larga maioria 87% está a encaminhar o tráfego DNS para outros servidores, o que requer a colaboração dos operadores dos servidores a jusante.

Apesar de prosseguir com estes trabalhos, a ICANN mantem incertezas à análise que efetuou, nomeadamente, em que medida a amostra de 0,57% é representativa do universo de todos os servidores resolvers, e como determinar o número de utilizadores e/ou sistemas que dependem de um servidor resolver.

Apesar de todos os esforços e vários anos de preparação, a ICANN revela-se ainda não completamente capaz de controlar o processo. A suspensão, inicialmente apenas por 3 meses, vai demorar tanto quanto o necessário para garantir que o número de utilizadores afetados pelo Rollover seja mínimo.

Atualmente, a ICANN continua a recolher dados e teme o efeito de reflexo, que possa originar a remoção da nova chave nos sistemas que já a conhecem.

PILOTO DE RDAP DO ICANN

O RDAP[20] foi desenvolvido para responder às lacunas do WHOIS, e apesar deste protocolo apresentar inúmeras vantagens sobre este último, a sua implementação não tem sido tão ágil como esperado. Entre os principais motivos de impasse, está a necessidade de clarificação de requisitos para determinados aspetos, nomeadamente o controlo de acesso à informação.

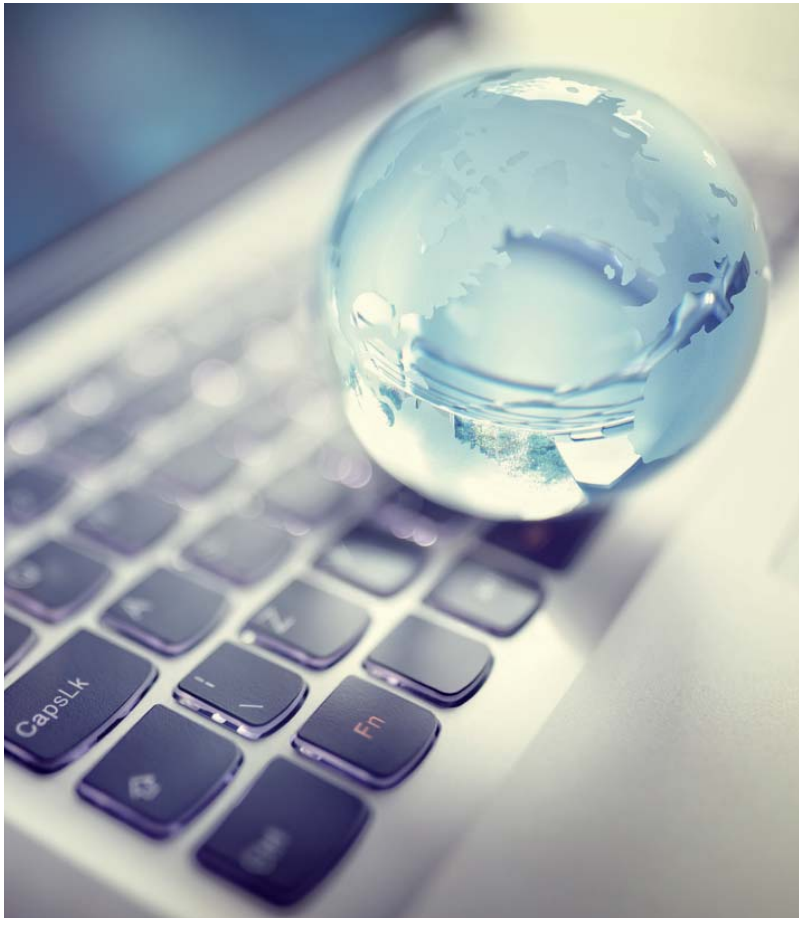
Na tentativa para desbloquear este impasse, a ICANN aceitou realizar um programa[21] piloto de RDAP, proposto[22] pelo *gTLD Registries Stakeholder Group (RySG)* com o suporte do *Registrar Stakeholder Group*.

O objetivo do programa piloto, é desenvolver um perfil (ou perfis) base para orientar a implementação de RDAP. Adicionalmente o programa deve definir uma data e um plano para implementação do serviço. É um programa de adesão voluntária, destina-se a entidades Registries e Registrars de gTLDs e decorre de 5 de setembro de 2017 até 31 de julho de 2018. Até ao momento os aderentes a este programa são a Google Registry com os seus 46 TLDs, a Afilias com .info, a Verisign com .com e o .net, e RyCE GmbH com .wien.

O RDAP já se encontra implementado em todos os Regional Internet Registries, RIRs, RIPE NCC, LACNIC, ARIN, APNIC e AfriNIC há vários anos.

20 *https://www.icann.org/rdap*
21 *https://www.icann.org/news/announcement-2017-09-05-en*
22 *https://www.icann.org/en/system/files/correspondence/diaz-to-atallah-03may17-en.pdf*

Nos ccTLDs, a implementação de RDAP faz-se ao ritmo definido por cada um. O .br, e o .cz foram dos primeiros a desenvolver implementações, ainda antes da publicação das especificações, RFC 7480 ao RFC 7485, pelo IETF em 2015.



PROJETO EBERO

Uma das inovações do programa de novos gTLDs foi a criação do programa *Emergency Back-End Registry Operators*, EBEROs. Trata-se de mecanismo que permite mitigar riscos da estabilidade e segurança do DNS, num cenário de falha de uma ou mais, funções criticas na operação de um novo gTLD.

Essas funções, são as seguintes:

- Resolução DNS
- Operação do registo e gestão de domínios (EPP)
- Operação de serviços RDS (Whois)
- Depósitos de Data Escrow
- Manutenção da zona devidamente assinada com DNSSEC

Até ao momento, não foi necessário ativar o programa EBERO numa situação real. Contudo, a ICANN aproveitou a suspensão de atividade de 3 gTLDs, para simular a execução do programa. Nestes 3 gTLDs , os respetivos Registries aceitaram a execução do programa, e cada teste foi feito com um operador EBERO distinto.

Quanto aos resultados dos testes efetuados, o menor tempo para reposição do serviço DNS foi de 11 horas e 55 minutos, já para os serviços de registo e WHOIS, o menor tempo foi de 2 dias, 5 horas e 5 minutos. No pior dos casos, todos os serviços foram restabelecidos em 8 dias.

Summary

Step	gTLD-1	gTLD-2	gTLD-3
Reached 100% of emergency threshold (Simulated)	16:00 UTC 26 Jan 2016	14:03 UTC 25 Apr 2017	00:05 UTC 21 Sep 2017
Total DNS downtime (simulated and discounting cache effects)	12 hours, 22 minutes	1 day, 9 hours, 5 minutes	11 hours, 55 minutes
Total RDDS downtime (simulated + real and discounting cache effects)	2 days, 5 hour, 5 minutes	3 day, 2 hours, 14 minutes	5 days, 17 hours, 58 minutes
Data Escrow function restored (End of exercise)	5 days, 21 hours, 53 minutes	8 days, 2 hours, 34 minutes	8 days, 3 hours, 21 minutes
Issues discovered	44 issues	37 issues	20 issues

https://schd.ws/hosted_files/icann60abudhabi2017/08/7%20EBERO%20Arias.pdf (pág.18)

Estes exercícios foram úteis para detetar e corrigir pequenas anomalias na execução dos processos, nomeadamente o acesso a chaves criptográficas, scripts com pequenos erros, entre outros.

Porem, é preciso notar, que os testes foram realizados com gTLDs praticamente vazios, sem domínios registados. Ficou por descobrir, quais seriam os tempos para a transição dos serviços de um gTLD com centenas ou milhares de domínios registados.

A ICANN monitoriza ativamente os gTLDs para garantir que estes cumprem os SLAs estabelecidos, caso tal não se verifique pode ser ativado o programa EBERO, assumindo a ICANN a operação destes. Porém, a ICANN tenta em primeiro lugar colaborar com o gTLD para corrigir a situação. Apesar de não existir nenhum caso real até à data, já houve mais de 30 de situações de "close call" em que esteve muito perto de acontecer.

No caso dos ccTLDs, cabe a cada um definir processos de continuidade de negócio para mitigar os riscos. Este é o caminho que o .pt tem feito nos últimos anos, estado atualmente a implementar uma solução de Disaster Recovery para assegurar a reposição dos serviços em caso de falha dos sistemas principais.

OUTROS TEMAS – EM DISCURSO DIRETO

Jacques Latour, apresentou a ideia de uma home network, onde todos os dispositivos IoT cada vez mais presentes no nosso dia-a-dia (em casa, no carro, telemóveis, gadgets, sensores no vestuário, sensores em equipamentos, etc) estariam ligados a uma única estrutura de controlo com foco na inovação e na automatização. Esta ideia foi bem recebida pela maioria dos presentes que se manifestaram.
Este conceito está especificado no draft-ietf-homenet-dot-14[23].

Ning Kong do CNNIC o Registry do .CN, apresentou a ideia de processar vários domínios em cadeia, a partir de um só domínio. Esta solução iria agilizar a configuração de vários domínios que partilham a mesma configuração, duma forma automática. Esta ideia não foi bem-recebida pela maioria dos presentes que se manifestaram. Este conceito está especificado no draft-yao-dnsext-bname-06[24].

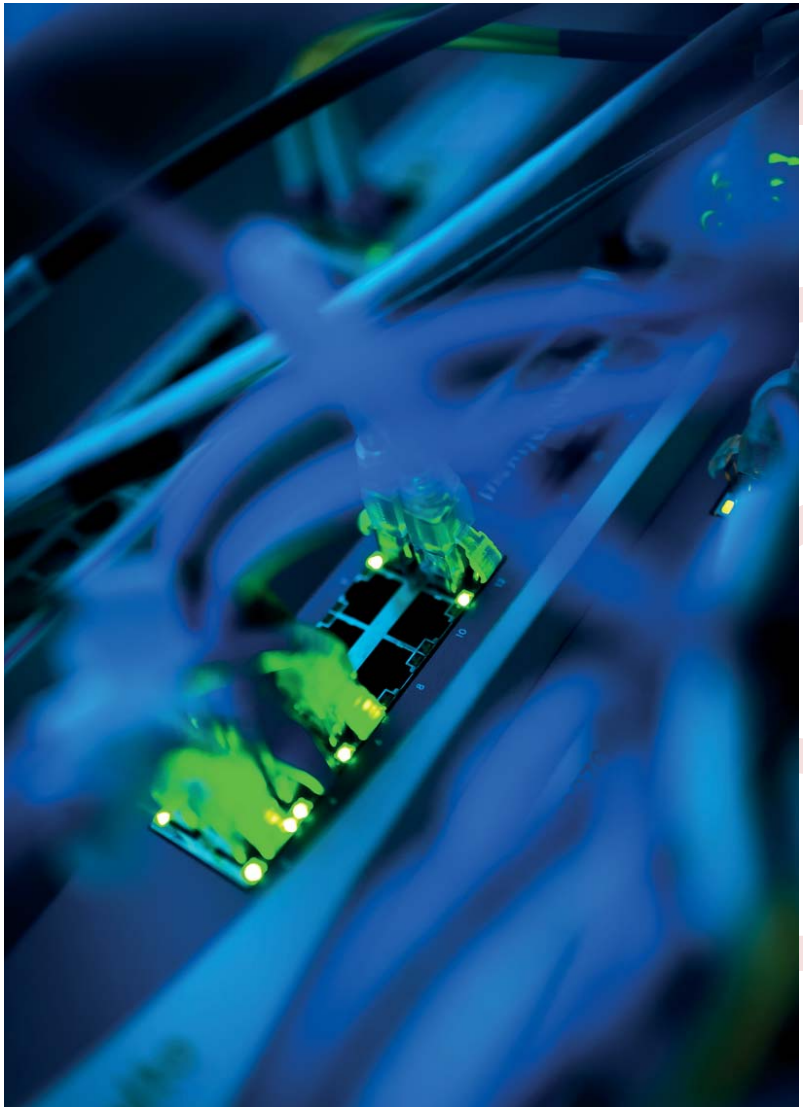
Ben McIlwain, engenheiro de software no Google, falou da importância de HTTP Strict Transport Security, HSTS, com preloading. Um mecanismo de politicas de segurança, que evita ataques como SSL-stripping man-in-the-middle e DNS Spoofing. Este mecanismo garante que a comunicação entre o servidor e o cliente apenas ocorre sobre um canal seguro com HTTPS.

23 *https://tools.ietf.org/html/draft-ietf-homenet-dot-14*
24 *https://www.ietf.org/internet-drafts/draft-yao-dnsext-bname-06.txt*

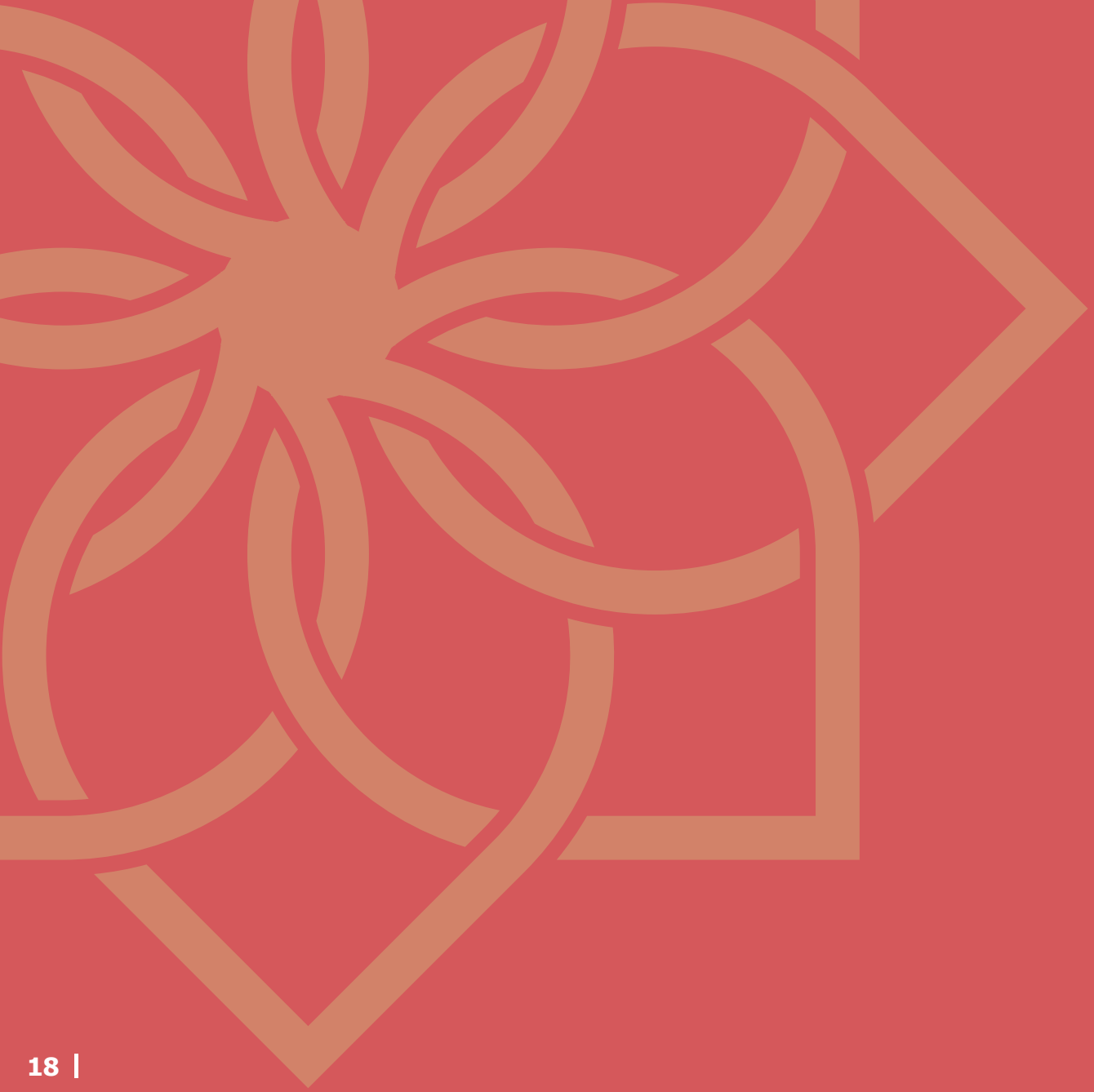
Dmitry Belyavskiy, do Technical Center of Internet, entidade responsável pela gestão técnica do ccTLD .ru, falou da atual compatibilidade de endereços de email com caracteres especiais, vulgo IDNs e certificados X.509. Dmitry referiu os desenvolvimentos das especificações no grupo de trabalho Email Address Internationalization, EAI no IETF, e o suporte aplicacional em soluções de servidor (Postfix 3.0+, Exim 4.86+, Dovecot e Roundcube) e soluções de clientes de email (Outlook 2016, iOS Mail, The Bat!).

Attila Özgit do ccTLD .TR, Turquia, falou do ataque informático perpetrado a 14 de dezembro de 2015, uma segunda-feira de manhã às 10:20, e com uma duração de quase 3 semanas. Numa primeira fase, tratou-se de um ataque de amplificação por DNS (UDP), realizado por botnets contra servidores resolver públicos e servidores autoritativos. Um segundo alvo foram os serviços de registo e gestão de domínios deste ccTLD. O ataque era mais ativo no horário de expediente, entre as 9:00 e as 17:00, nos restantes horários reduzia o volume. A determinada altura um ISP reportou 220 Gbps de largura de banda utilizada pelo ataque. Em resposta o .TR aumentou a capacidade de servidores de nomes, e começou a analisar o tráfego DNS para determinar regras de exclusão.

Esta ocorrência revelou a importância de mecanismos expeditos na atualização da zona raiz pela IANA, e a necessidade de mecanismos de comunicação ágeis e eficazes, entre todas as partes envolvidas, nomeadamente Registry e os ISPs.



ICANN | 60 • DNSSEC



Na apresentação de entrada, Jacques Latour do .CA mostrou uma atualização dos números da implementação DNSSEC. Em termos globais a validação DNSSEC baixou ligeiramente no 2º quadrimestre situando-se agora perto dos 11%. Este valor é praticamente assegurado na integra pelo serviço Public DNS do Google. Em termos regionais a África Austral é a região que detém a maior taxa de validação DNSSEC com 38% porém, destes, 19,67% são assegurados pelo Google. Por último, considerando a região do médio oriente, o Iraque destaca-se com a validação DNSSEC de 57,38% do tráfego DNS, dos quais 25,54% são assegurados pelo Google.

No universo de 1541 TLDs, 1394 estão assinados com DNSSEC. O .gw, ccTLD da Guiné Bissau, foi o mais recente a ser assinado, tarefa executada pelo DNS.PT enquanto responsável pela gestão técnica do .gw. Porém, como referido em relatórios de ICANNs anteriores, África continua a ser a região geográfica onde continua a haver muito trabalho por fazer, para uma adoção plena de DNSSEC.

Na região do medio oriente, o .SA, ccTLD da Arabia Saudita, foi o primeiro ccTLD a implementar DNSSEC, tendo assinado em junho. Outros ccTLDs da região estão a trabalhar na implementação de DNSSEC, nomeadamente o Iraque, o Irão, a Síria, o Azerbaijão. Na Turquia os trabalhos em DNSSEC têm-se centrado na sensibilização via ações de formação. Segundo Kadir Erdogan, a comunidade Turca reconhece a importância de DNSSEC, porém os decisores chave não tomam a decisão de avançar para a respetiva implementação.

Depois da ICANN ter suspenso o Rollover da Root, foram vários os projetos e iniciativas da comunidade que surgiram para ajudar a analisar parâmetros internet que possam influenciar neste campo.

O projeto Root Canary apresentado por Cristian Hesselman do SIDN registry do ccTLD .NL, é um desses projetos. Tem por objetivo reunir vários indicadores associados ao Rollover, duma perspetiva global, de forma a construir uma base de conhecimentos sólida sobre este tipo de eventos.

O projeto Root Canary utiliza várias fontes de indicadores, nomeadamente os projetos Ripe Atlas, Luminati, APNIC DNSSEC measurement e também o tráfego DNS observado em vários servidores raiz.

Também dentro da temática do Rollover, Geoff Huston da APNIC, apresentou o trabalho que está a desenvolver juntamente com o consultor do DNS.PT, João Damas. Este trabalho é particularmente interessante, porque ao contrário das restantes iniciativas, incluindo a da ICANN, o focus não está nos servidores de Resolver, mas sim nos utilizadores. Segundo Geoff Huston, o resolver da Google resolve cerca de 14% do tráfego DNSSEC mundial, contudo os resolvers que cada utilizador tem em casa, apenas resolve o tráfego gerado por cada um de nós. Logo é necessário ter visibilidade da Infraestrutura do lado do utilizador.

A solução proposta denominada por "A Sentinel for Detecting Trusted Keys in DNSSEC" encontra-se documentada e publicada no documento "draft-huston-kskroll-sentinel-02.txt".

dns.pt
dnssec.pt
facebook.com/dns.pt
pt.linkedin.com/in/dnspt

Produção: novembro 2017
Grafismo: dns.pt