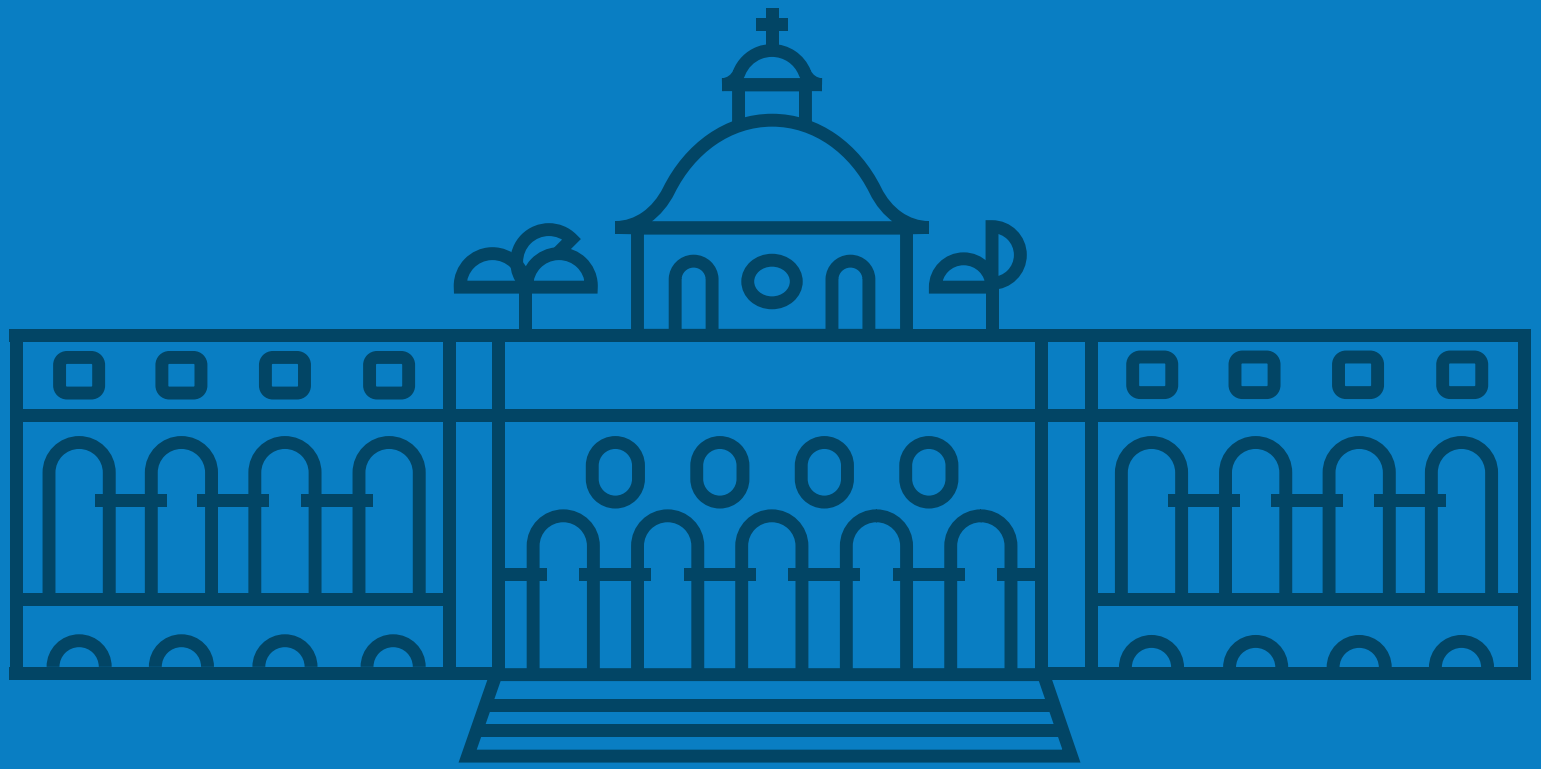
ICANN 61
COMMUNITY FORUM

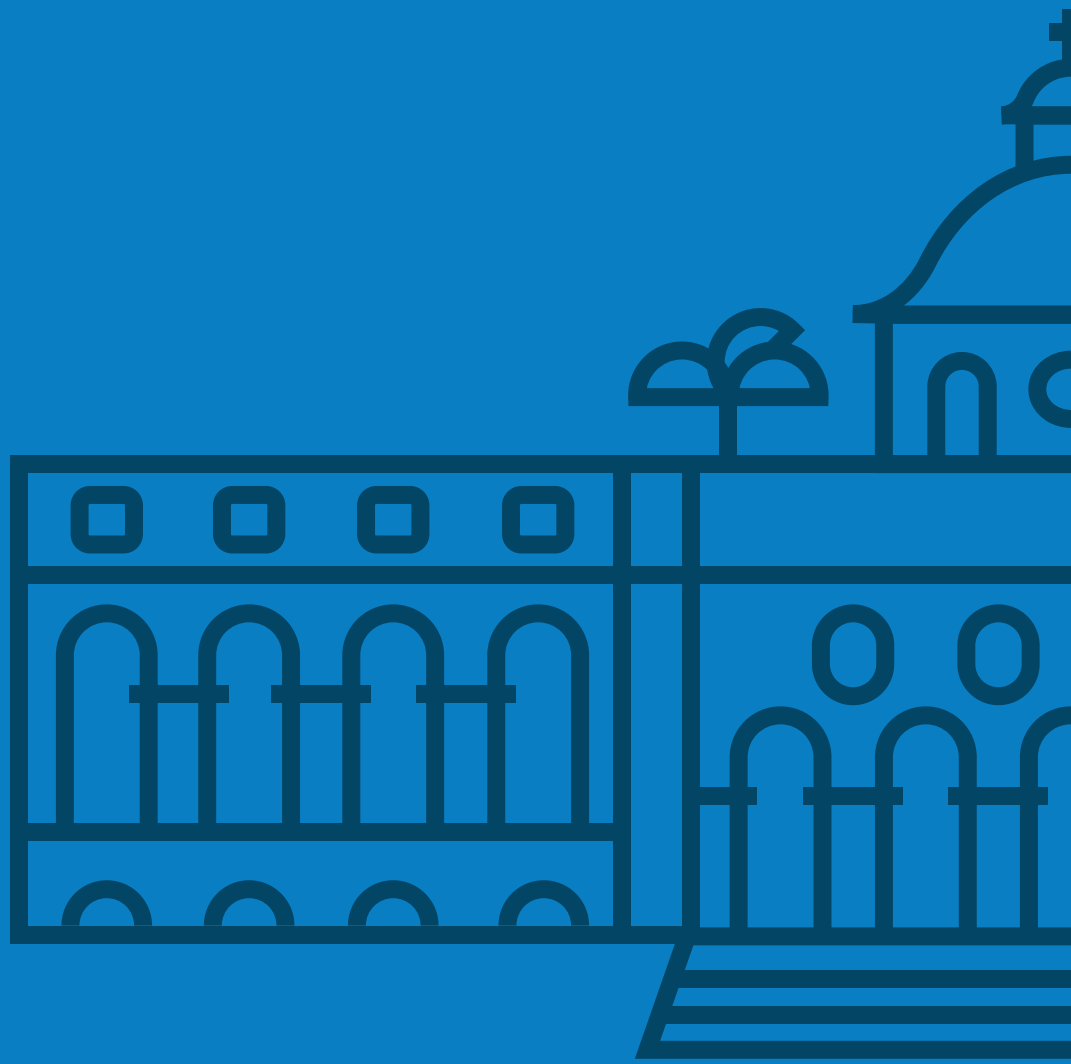
SAN JUAN
10–15 March 2018

DNS-OARC28

RELATÓRIO TÉCNICO DNS.PT

ÍNDICE





DNS OARC 28
8 E 9 DE MARÇO DE 2018 - SAN JUAN, PORTO RICO

O DNS OARC 28 realizou-se em San Juan, Porto Rico durante os dias 8 e 9 de março de 2018. O evento iniciou com o habitual relatório da equipa do DNS-OARC nas suas diferentes vertentes.

De destacar o *update* feito no software que o DNS-OARC mantém, nomeadamente o DNSJIT que poderá ser usado em experiências futuras no DNS.PT.

A manhã do primeiro dia terminou com as duas primeiras apresentações públicas do Workshop, estando a primeira a cargo do Facebook que apresentou a sua infraestrutura pública e privada de DNS. Na segunda apresentação falou-se da problemática relativa aos dispositivos que a maior parte dos ISP's instalam nos clientes, que não permitem alterar os servidores de DNS. Não é sabido, por parte da comunidade, o porquê desta limitação mas, aparentemente, trata-se de uma questão de simplificação de forma para que o cliente não cometa erros e não ligue para o suporte técnico com um problema que o próprio criou.

A sessão da tarde iniciou com uma apresentação por parte da SalesForce, sobre como múltiplos fornecedores de serviços de DNS suportam DNSSEC em zonas que partilham entre si. Os resultados foram positivos, mas não o suficiente para se afirmar que os múltiplos fornecedores suportam DNSSEC num sistema de partilha de chaves.

A apresentação seguinte focou-se em medir a eficiência de um protocolo recente descrito no RFC8198, o *Aggressive Use of DNSSEC-Validated Cache*. Os resultados do estudo apresentado foram bastante positivos, apresentando-se este método, como forma excelente de mitigar um dos ataques comuns no DNS, o *Randon Subdomain Atack*.

A terceira apresentação colocou em evidência um problema existente no atual sistema de rotação do algoritmo de síntese (DS) de uma chave DNSSEC na zona pai. O orador recorreu à exposição de um caso prático para demonstrar que, o RFC que descreve esta rotação tem um erro que provoca indisponibilidade da zona se o mesmo for seguido à risca.

Foi, contudo, salientado que atualmente se encontram a explorar uma forma de correção ao RFC para que a referida situação não tenha impactos consideráveis.

A última apresentação deste painel focou-se em como a Comcast, operador de telecomunicações americano, utiliza *Negative Trust Anchors* para resolver, temporariamente, questões de falha de DNSSEC que acontecem, por vezes, em alguns sites de elevada importância.

O *Negative Trust Anchors* é uma tecnologia que permite configurar um *resolver* para ignorar uma falha no DNSSEC, num determinado domínio. É necessário recorrer a esta tecnologia quando, por vezes, sites de elevada importância começam a falhar por um erro de DNSSEC (ex: expiração de chaves DNSSEC).

A sessão da tarde encerrou com duas apresentações, uma sobre o BIND 9 e outra do DNS-OARC.

Na apresentação do BIND 9 foram elencados os *updates* que têm sido feitos a este software e o *road map* de desenvolvimentos que ocorrerão.

Por fim, o DNS-OARC apresentou uma ferramenta que está a desenvolver, o DNSJIT. Esta ferramenta junta um conjunto de outras do DNS-OARC que procedem à recolha, análise e *replay* de tráfego e estatísticas sobre o tráfego de um servidor de DNS. Esta ferramenta pode ser bastante útil em trabalhos de investigação que o DNS.PT possa vir a desenvolver.

O segundo dia do DNS-OARC 28 foi iniciado com uma sessão dedicada ao DNSSEC.

A primeira apresentação esteve a cargo da ICANN, que expos os planos para prosseguir com o *rollover* da KSK da raiz do DNS.

Nesta fase a ICANN encontra-se a aguardar comentários por parte da comunidade sobre o plano que publicaram, propondo-se a dar seguimento ao *rollover* a 11 de outubro de 2018.

A segunda apresentação da manhã colocou em evidência um protocolo que se encontra a ser desenvolvido e cujo intuito é medir a preparação da internet para a rotação da chave da raiz, tendo como foco os utilizadores.

Uma das fragilidades dos atuais protocolos que tentam medir a preparação da internet para a rotação da chave é o facto de estes terem como foco os *resolvers* e não os utilizadores, existindo o problema de não se saber quantos utilizadores estão por detrás destes *resolvers* não sendo, por isso, possível aferir quantos utilizadores serão afetados pela rotação de forma negativa.

A última apresentação do painel partilhou um estudo sobre a preparação de alguns *resolvers* para receber o RFC 5011.

Este estudo descreve o procedimento de rotação de chave na root e a razão pelo qual os *resolvers* confiam na nova chave.

Foi possível constatar que a maior parte dos softwares testados suportam este RFC de forma quase standard, tendo existido alguns problemas ao longo do desenvolvimento dos softwares e nas várias versões lançadas.

A principal conclusão que é possível retirar do estudo apresentado, assenta na premissa de que todos os utilizadores da internet devem fazer um *update* aos softwares que habitualmente usam, para terem sempre a versão mais atualizada.

O segundo painel da manhã iniciou com uma apresentação da LACNIC, na qual se tentou identificar *openresolvers* de DNS a correr sobre IPV6.

A identificação de *openresolvers* no espaço de endereçamento IPv6 revela-se, à partida, difícil de acontecer atendendo a que o espaço de endereçamento é bastante grande, não sendo possível percorrê-lo em tempo útil.

Desta forma, foi criado um mecanismo de identificação de *resolvers* usando os servidores autoritativos do LACNIC. Foi, ainda, realizado um estudo com o intuito de perceber se os mesmos seriam considerados *openresolvers*.

Apesar de o estudo ainda se encontrar a decorrer, é possível verificar, através de resultados preliminares, a existência de um número, não muito elevado, de *openresolvers* face ao total de servidores.

Na segunda apresentação do painel, a ICANN partilhou um estudo que demonstra que os *root-servers* são atingidos por *queries*, algo que não deveria acontecer.

Para a realização deste estudo, a ICANN recorreu aos dados recolhidos no DITL 2017 (Day-In-The-Life), que o DNS-OARC reúne anualmente.

Foi possível concluir que existe um conjunto de *queries* que chegam aos *root-servers*, sendo que tal não deveria acontecer, tendo ainda sido possível identificar um outro conjunto de novas *queries*.

De todo o tráfego analisado, o principal tráfego anómalo identificado reside num conjunto de *queries* para TLDs com um formato aleatório.

Não se compreende, na totalidade, a origem destas *queries* mas acredita-se que possam ser sistemas maliciosos ou sistemas de sinalização.

A última apresentação da manhã incidiu sobre um estudo atinente à eficiência do *Anycast* num *root-server*.

Através deste estudo foi preciso concluir que a referida eficiência é bastante positiva, existindo um número muito reduzido de *queries* que não optam pelo caminho que seria de esperar, isto é, pelo caminho mais curto.

A sessão da tarde iniciou com a apresentação de um novo protocolo que está em desenvolvimento, o ATR (Additional Truncated Response).

Uma das fragilidades do DNS reside no facto de que as grandes respostas, muitas vezes, não chegam aos utilizadores, devido a problemas na rede e/ou configurações defeituosas.

O ATR combate a perda destas respostas introduzindo um novo pacote, mais pequeno, que à partida os servidores conseguem receber.

Foram feitos alguns estudos sobre este novo protocolo e os resultados têm sido bastante positivos. O protocolo está, neste momento, em fase de revisão e aprovação pela comunidade e prevê-se que comece a ser implementado brevemente.

Seguiu-se um *update* à tentativa de introdução de múltiplas respostas num pacote de DNS. Atualmente, o DNS é um serviço de pedido e resposta única, contudo, desde o início que está previsto que possam existir múltiplos pedidos e respostas, apesar de não existirem muitas soluções que o consigam assegurar.

A última apresentação deste painel introduziu uma nova solução para a anonimização do DNS. Nesta solução, o sistema normal de DNS é usado para criar um domínio especial que, por sua vez, é usado para encriptar a comunicação entre o utilizador e o resolver. Desta forma, e utilizando o sistema de DNS normal, é possível encriptar as *queries* realizadas.

Apesar de ainda se encontrar numa fase inicial e de ser um protótipo, esta solução tem apresentado resultados bastante interessantes.

O último painel iniciou com uma apresentação que carateriza o tráfego de DNS dentro da rede TOR.

A rede TOR é uma rede paralela que funciona em cima da internet normal, mas que esconde o tráfego do utilizador evitando, assim, possíveis bloqueios na rede. Foi apresentado um estudo, através do qual se tentou apurar o quão anónimo é o tráfego de DNS que um utilizador produz. Os resultados obtidos são positivos, apesar da lentidão da rede, conseguindo o utilizador um bom nível de anonimização.

A última apresentação do workshop fez referência a um estudo comparativo entre os vários mecanismos que existem atualmente e que tentam manter a privacidade no tráfego de DNS que é enviado para os diferentes atores do mesmo, sendo que o foco principal do estudo residia em verificar qual a melhor opção para anonimizar o tráfego enviado para a raiz do DNS.

De todos os métodos estudados, aquele que apresenta melhores resultados é a existência de um cópia local no *resolver* da raiz do DNS, que faz com que nenhum tráfego para este ponto saia da rede local e, também, que exista um aumento na performance do sistema.

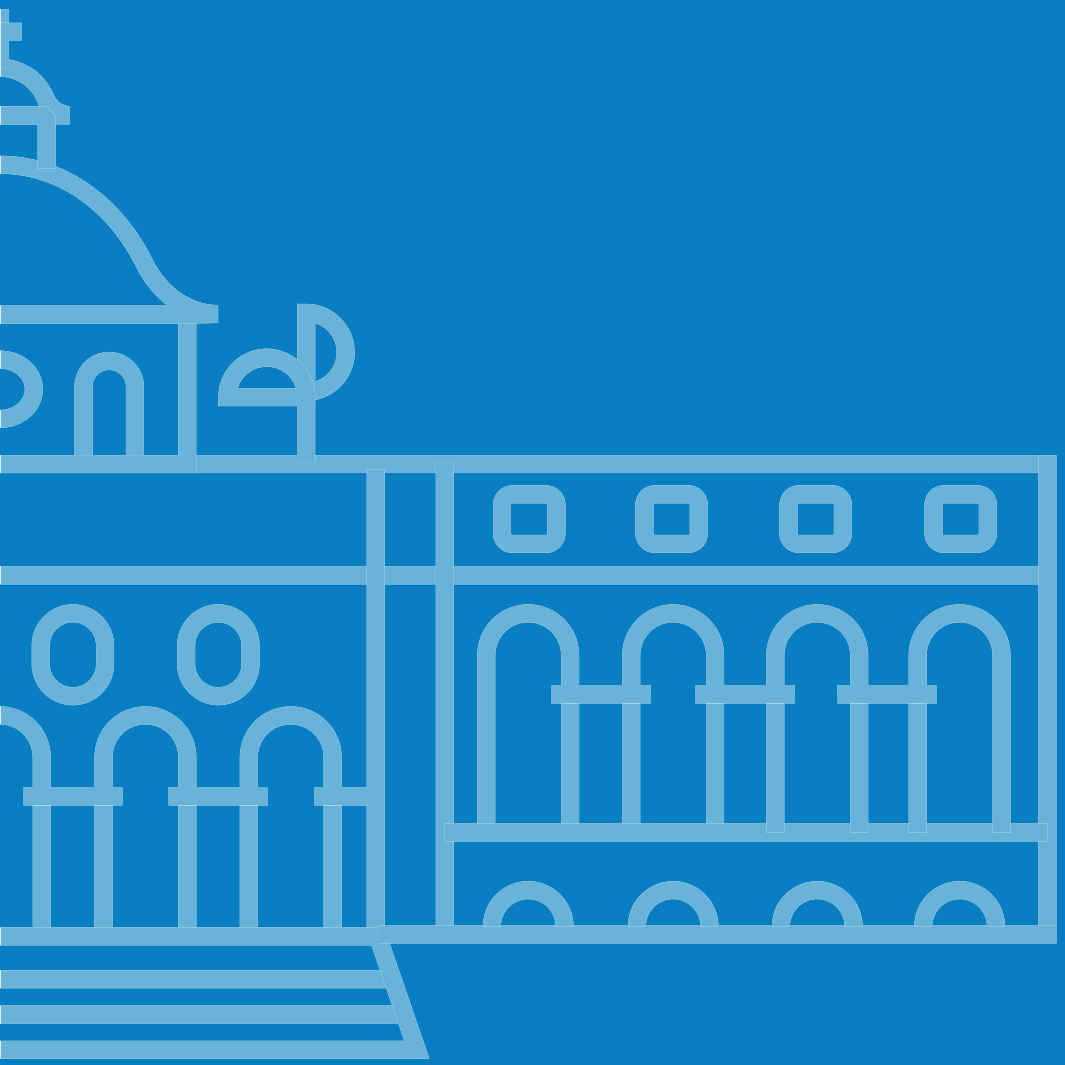
Por fim, houve, ainda, tempo para "*lightning talks*".

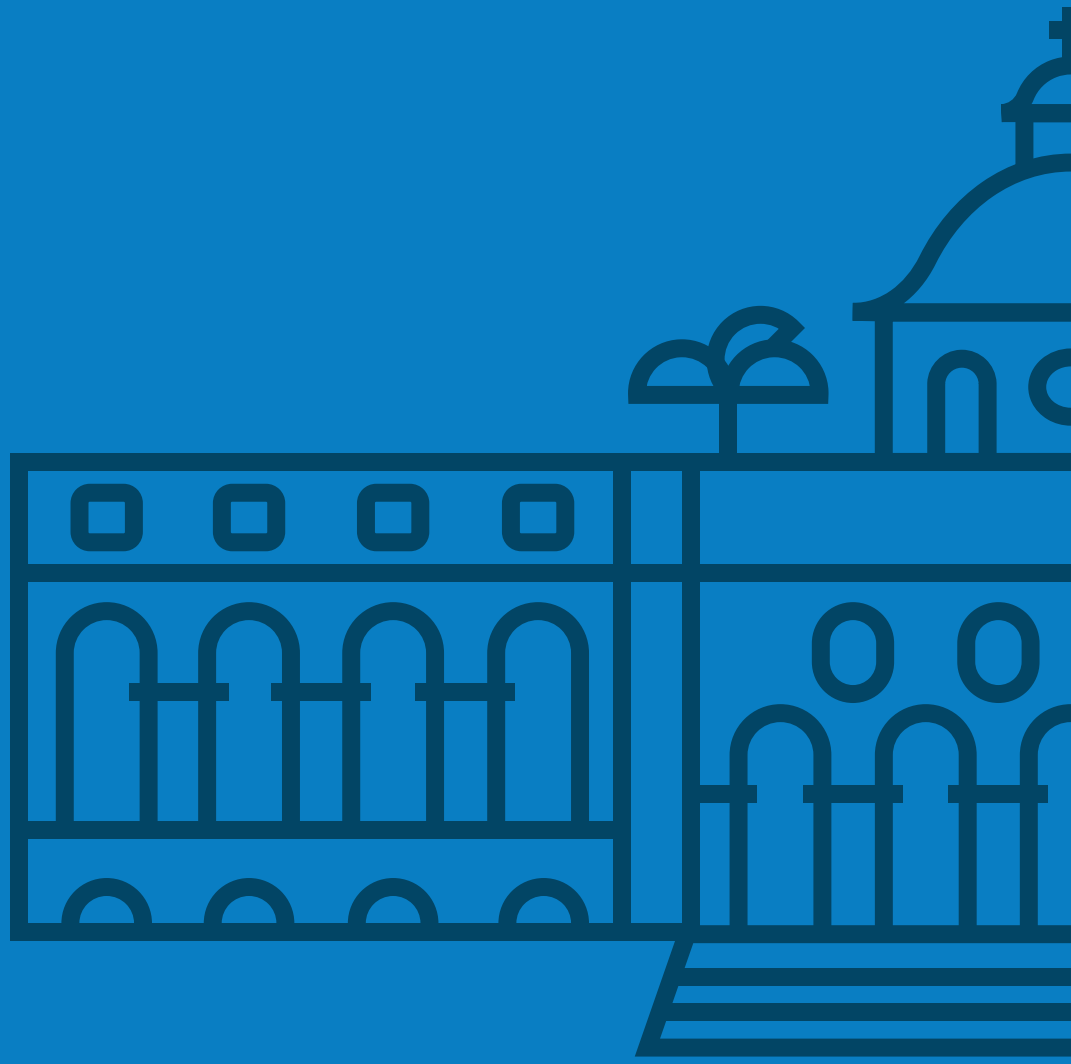
De todas as apresentações feitas neste âmbito, há duas que merecem ser destacadas.

A primeira relativa à apresentação de um estudo sobre como a recente descoberta de bugs nos sistemas INTEL afetou o desempenho do BIND. Os resultados apresentados evidenciaram que não houve uma degradação muito significativa, especialmente em comparação a outros sistemas.

A segunda apresentação que destacamos referiu os diversos *workarrounds* que os softwares de DNS têm implementados, devido a questões de implementação do EDNS. Aqui os fabricantes de software anunciaram uma iniciativa para descontinuar estes *workarrounds* deixando, assim, que software potencialmente desatualizado deixe de funcionar.

ICANN | 61





ICANN 61
10 A 15 DE MARÇO DE 2018 - SAN JUAN, PORTO RICO

Entre 10 e 15 de março em San Juan, Porto Rico, teve lugar o ICANN 61, fórum que reúne os mais diversos grupos de pessoas com interesse na Governação da Internet e com especial incidência na governação e funcionamento do sistema de DNS, um dos sistemas principais pilares para o bom funcionamento da internet global.

Como já é habitual, o DNS.PT acompanhou com elevado interesse os fóruns que decorreram neste evento, com especial destaque para o Tech Day e para o DNSSEC Workshop.

ICANN 61 EM NÚMEROS

1,565 CHECKED-IN PARTICIPANTS, WITH **604** LISTING THEIR REGION AS NORTH AMERICA

36% OF ATTENDEES PARTICIPATING FOR THE FIRST TIME

342 SESSIONS HELD, FOR A TOTAL OF **630.5** HOURS

167,907 SCHEDULE PLATFORM PAGE VIEWS, A **198%** INCREASE FROM ICANN60 ABU DHABI

11,106 GIGABYTES OF DATA AS NETWORK TRAFFIC

14% OF NETWORK TRAFFIC WAS INTERNET PROTOCOL VERSION 6 (IPV6), A **1%** INCREASE FROM ICANN60 ABU DHABI

A abertura do Tech Day pautou-se pela apresentação, por parte de um representante do SSAC (Security and Stability Advisory Committee), da possibilidade de serem usados Emojis nos nomes de domínios, em qualquer ponto da árvore.

Após inúmeros testes realizados, foi possível concluir que os Emojis podem ser bastante complexos, apresentando diversas variantes não standard, tornando o seu uso no DNS desaconselhado.

Atendendo a esta questão e acrescendo ainda as ameaças que estes podem constituir para o bom funcionamento do sistema, o SSAC, irá recomendar, ao Board da ICANN, que não permita o uso deste tipo de caracteres na Raiz do DNS, ou em qualquer outro ponto da árvore.

Seguiu-se a apresentação do projeto LocalRoot.
O sistema DNS tem, no topo, o ponto (.) que é a raiz do DNS, existindo inúmeras cópias destes servidores a nível mundial. Os IP's das treze cópias dos servidores raiz são compilados no código de todos os *resolvers* a nível mundial e são o ponto de partida para o início da resolução de DNS.

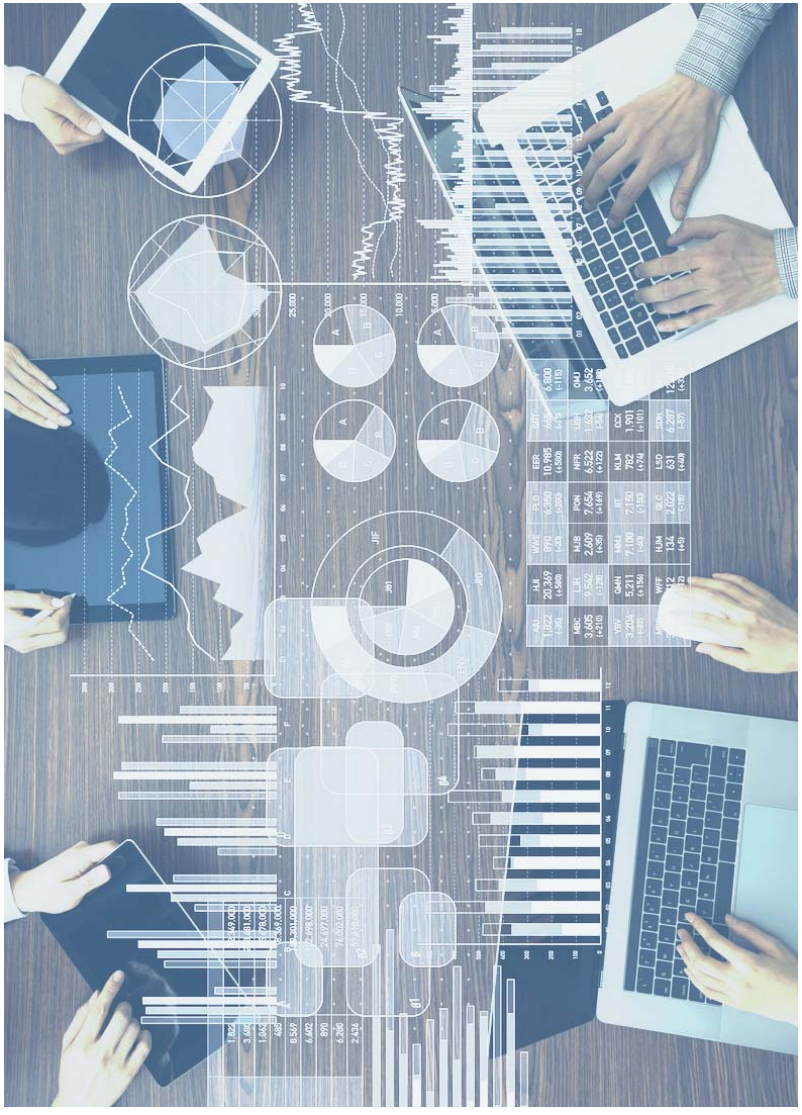
Apresentando-se como um sistema crítico e altamente distribuído, este sistema é, também, muito suscetível de ser atacado podendo, no limite, ficar indisponível. Uma das formas de tentar minimizar esta vulnerabilidade do sistema traduz-se em criar uma cópia local nos *resolvers* da zona raiz.

Foi com esse propósito que surgiu o projeto LocalRoot, que dá resposta a esta necessidade ao permitir que os *resolvers* tenham uma cópia local da zona raiz sempre atualizada. Para além da proteção contra uma possível falha do sistema global, este sistema diminui, também, o tempo de resolução de um domínio, uma vez que possibilita a utilização da cópia local da zona raiz, não sendo necessário contactar um servidor global e, por isso, sujeitar-se à latência de rede adicionada ao tempo global da *query*.

Por fim, a última apresentação deu a conhecer o D-Zone DNS Firewall, um serviço acabado de lançar pelo CIRA, registry canadiano (CIRA).

O D-Zone DNS Firewall disponibiliza aos diversos clientes um serviço de resolver de DNS com proteção ao nível das respostas. Esta proteção designa-se de DNS RPZ que, tendo em conta um conjunto de feed's, bloqueia diversos sites com "má reputação" pelos mais diversos motivos (conteúdo malicioso, malware, etc).

Este serviço foi implementado pela CIRA numa tentativa de diversificar a oferta. Surgiram, contudo, alguns problemas na implementação do mesmo atendendo aos elevados volumes de tráfego dos serviços recursivos. Foi, por isso, necessário adaptar a sua estratégia ao longo do tempo de implementação do projeto.



A sessão da tarde começou com uma apresentação conduzida pelo anfitrião, o NIC.PR.

Como é do conhecimento geral, Porto Rico passou recentemente por um evento catastrófico que fez com que a ilha estivesse praticamente um mês em estado de emergência.

Na sua apresentação, o NIC.PR falou sobre a ativação do plano de Disaster Recovery (DR) e a forma como sobreviveu, durante algum tempo, em condições limitadas.

Na operação do NIC.PR os efeitos do desastre natural foram diminutos, devido ao seu plano de ações devidamente estruturado. No entanto, a organização deverá manter-se atenta uma vez que, tal como foi referido, prevê-se que este tipo de desastres ocorra com maior frequência e com um impacto mais significativo nas organizações.

Para além de assegurar a continuação da operação em situação de emergência, o registry focou-se, ainda, em tentar ajudar a sociedade na sua recuperação.

Neste sentido foram desenvolvidas duas atividades: a criação do website http://status.pr/, no qual é possível aferir o grau de recuperação das infraestruturas do país e, por outro lado, não deixar expirar os domínios até que o país recupere da catástrofe, garantindo o funcionamento de empresas ou websites da região.

A apresentação seguinte incidiu sobre um protocolo que se encontra ser desenvolvido e que pretende medir a preparação da internet para a rotação da chave da raiz, tendo como foco os utilizadores.

Uma das limitações dos atuais protocolos que tentam medir a disponibilidade da internet para a rotação da chave reside no facto de terem como foco os resolvers e não os utilizadores. Tal representa uma entrave na medida em que não se sabe quantos utilizadores estão por detrás destes resolvers, não sendo possível aferir quantos utilizadores serão afetados pela rotação de forma negativa.

Por último, foi abordado o projeto Loon da Google.
Este projeto tem como objetivo aumentar a conectividade no mundo, especialmente em locais remotos, recorrendo a balões de elevada altitude.

Estes balões conseguem fornecer não só internet mas, também, comunicações móveis, o que reveste uma extrema importância em caso de catástrofe. Tendo sido iniciado há já algum tempo, este projeto tem vindo a desenvolver-se bastante ao longo dos últimos tempos, com especial sucesso em localizações remotas ou com acesso limitado, bem como em locais afetados por catástrofes naturais. O caso da catástrofe ocorrida em Porto Rico é um excelente exemplo disso, na medida em que estes balões ajudaram a restabelecer rapidamente as comunicações sem necessidade de colocar torres de comunicações em funcionamento.

O painel de abertura da última sessão do Tech Day abordou a problemática da aceitação universal na internet.

A internet começou por ser implementada no ocidente, tendo a mesma sido desenvolvida para o conjunto de caracteres universais, não considerando outros tipos de línguas e conjuntos de caracteres existentes no mundo.

Para acompanhar esta questão, foi formado, dentro da ICANN, um grupo sobre aceitação universal designado por USAG (Universal Acceptance), que tem vindo a acompanhar e a traçar objetivos sobre como este problema poderá ser abordado e melhorado.

No decorrer da apresentação foi feito um ponto de situação sobre o acompanhamento e desenvolvimento deste tema.

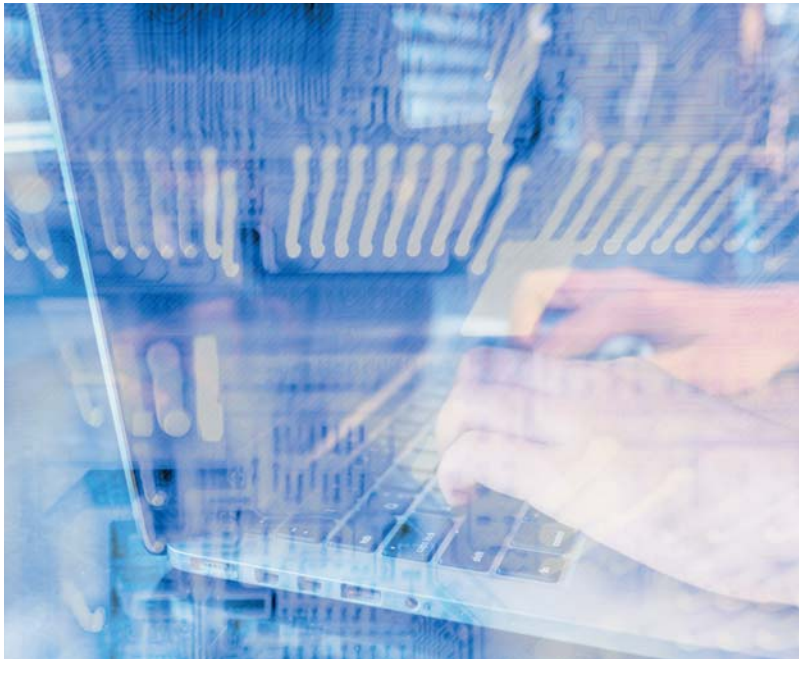
Posteriormente, foi feito um *update* sobre o sistema de registo desenvolvido pelo registry checo, o FRED.

O FRED é um sistema de gestão e registo de nomes de domínios *open source* que tem alguma aceitação em mercados específicos e que tem sofrido atualizações constantes.

No seguimento da sessão, foi discutida a problemática dos domínios IDN homógrafos que ainda se revelam um problema na internet.

Estes domínios têm, para o utilizador, um formato semelhante aos domínios usuais e são tipicamente utilizados para *phishing* ou outras atividades maliciosas. Tendo em conta que, esta problemática já existe praticamente desde o inicio da internet, do ponto de vista comercial seria de esperar que a mesma já fosse pouco relevante, no entanto o estudo apresentado mostra que este tipo de domínios ainda é usado para práticas ilícitas.

Concluiu-se sobre a necessidade de promover uma ação, ao nível da Governação da Internet, de forma a reduzir o uso destes domínios e o seu impacto atualmente.



Por último, a CIRA, registry canadiano, deu a conhecer o seu posicionamento sobre a problemática dos dispositivos de IOT (Internet of Things) que existem atualmente e que podem provocar constrangimentos na internet atual.

Os sistemas de IOT existentes, e que as pessoas facilmente usam em casa, têm como fragilidade o facto de poderem ser usados de forma menos própria, já que apresentam níveis de segurança extremamente baixos. Assim, a CIRA, apresentou um modelo que está a desenvolver, no qual os *routers* de cada habitação são inteligentes, apercebendo-se da existência de dispositivos IOT na rede e que não deveriam ter acesso à internet e à rede no geral, conseguindo proteger, assim, a internet.

O DNSSEC Workshop iniciou com o habitual ponto de situação sobre a implementação de DNSSEC no mundo.
Os números apresentados refletem um aumento da sua implementação a nível global, apesar de revelarem que alguns ISP's desligaram a validação devido ao receio gerado pela rotação da chave, que se prevê que se concretize este ano.

A sessão da manhã foi dedicada a um painel com o intuito de discutir as diversas atividades de DNSSEC que têm ocorrido pelo mundo, nomeadamente no Canadá, em Porto Rico e no Brasil.

No Canadá é possível verificar uma certa evolução no número de domínios assinados, ainda que muito lenta, registando-se um pequeno decréscimo ao nível da validação.

No que às atividades do registry diz respeito, não houve grandes alterações, justificadas pelo facto deste se encontrar focado noutras atividades.

O TLD de Porto Rico foi assinado, pela primeira vez, em 2006 tendo sido o segundo a assinar o domínio. Existem, contudo, poucos domínios assinados, e os que há são, essencialmente, do governo local. O registry tem promovido continuamente a assinatura de domínios.

Por fim, o Brasil falou sobre os planos para o RollOver de algoritmo que tem preparado para este ano e que iniciará brevemente.

Durante o Workshop foi, ainda, feita referência ao projeto, já apresentado no Tech Day, sobre a medição da preparação da rotação das chaves da root.

Seguiu-se mais um *update* sobre o projeto Turris do CZ.NIC, um projeto no qual o registry Checo tem que produzir routers de acesso doméstico mais baratos e funcionais e com funcionalidades de segurança asseguradas.

O registry Checo tem tido bastante sucesso neste projeto, tendo descoberto inúmeras questões ao ativar a validação DNSSEC, por defeito, nestes equipamentos.

Desta forma, e nas diversas evoluções que o projeto teve, o registry tem trabalhado no sentido de evoluir o sistema para que este tenha testes automáticos, para que possa detetar problemas nas redes dos operadores e, também, para que consiga autorregenerar-se de forma a melhorar o acesso à internet dos utilizadores que compraram este dispositivo.

Na apresentação seguinte o registry canadiano, CIRA, apresentou as alterações à sua infraestrutura de geração e assinatura DNSSEC da zona .CA.

Inicialmente o processo de geração de zona era bastante arcaico e demorado. Ao longo dos últimos meses o .CA alterou a metodologia deste processo, melhorando-o e tornando-o mais rápido, passando a demorar agora metade do tempo original.

Na última apresentação da manhã a Comcast, ISP americano, falou da sua experiência com o NTA (Negative Trust Anchors).

A Comcast tem validação DNSSEC implementada há bastante tempo na sua rede de resolvers, sendo que um dos problemas evidenciados está relacionado com a assinatura de domínios. Esta questão é da responsabilidade do titular do site contudo acaba por afetar, por vezes, a imagem do ISP. Desta forma, foi criada a NTA que permite desativar a validação DNSSEC para um determinado site, por um período limitado de tempo, e permitir o acesso ao site apesar da validação DNSSEC estar a falhar.

A Comcast tem o NTA ativo e a funcionar, recebendo alertas sempre que um site começar a falhar e determinando, à posteriori, se a sua visibilidade é suficiente para ser colocado na lista de NTA temporariamente, até o dono do site resolver a questão.

Nesta apresentação referiram, ainda, a experiência que tiveram com NTA e sobre os resultados positivos que a mesma tem tido.

A sessão da tarde do DNSSEC Workshop iniciou com uma apresentação sobre como o DANE torna o email mais seguro.

DANE é uma tecnologia na qual são publicados, no DNS, resumos dos certificados digitais usados para comunicação segura. Desta forma, e para além da confiança dada pela emissão de certificados pela CA, o sistema de DNS também confere segurança aos certificados.

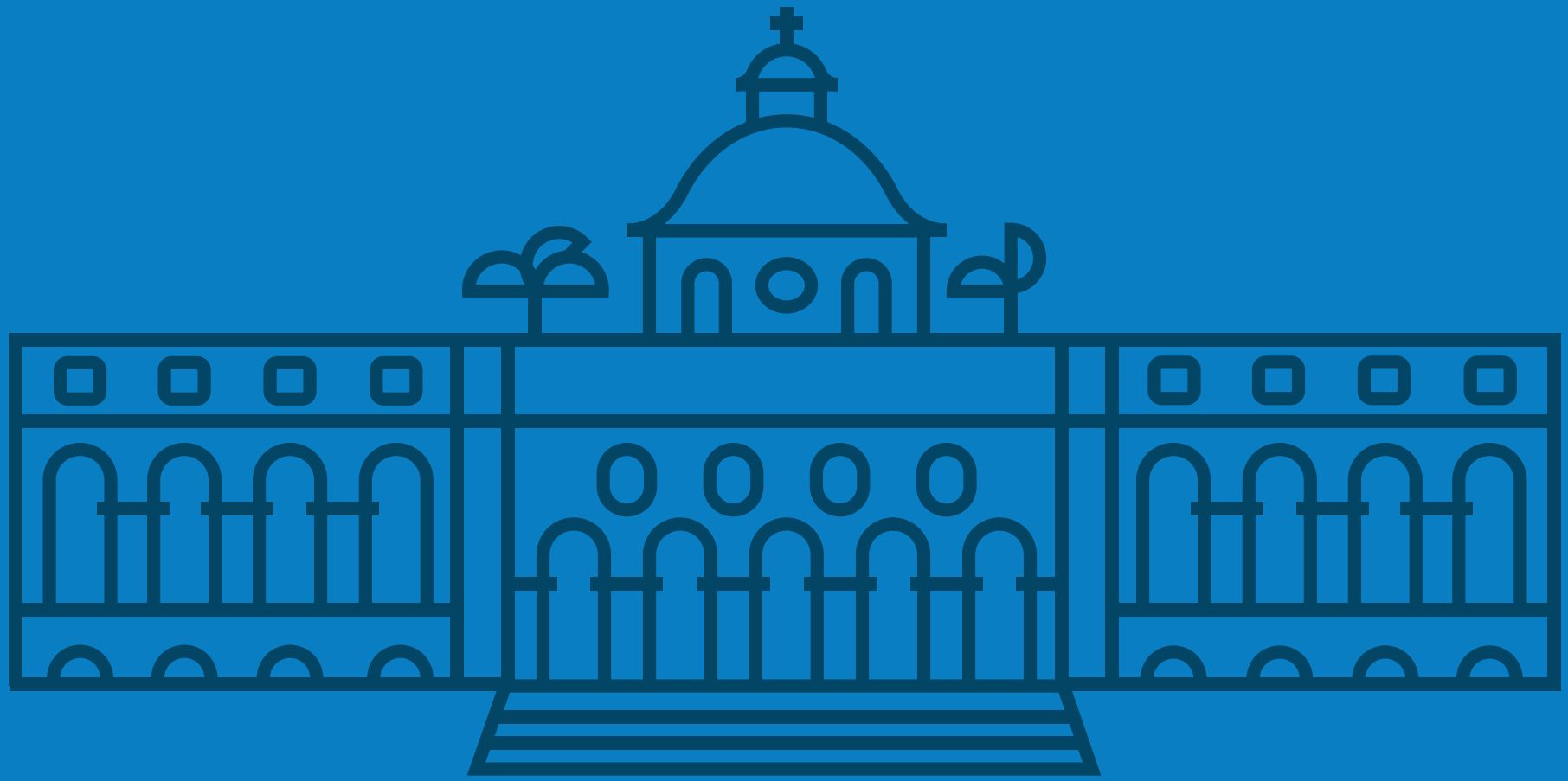
Ao usar DANE para validar os certificados digitais usados para as MTA's comunicarem, adiciona-se um nível de segurança, para além do email, já que a comunicação neste canal está sujeita a ataques que, de outra forma, não poderiam ser mitigados.

Por último, no Workshop foram abordadas as pretensões do ICANN em continuar com a rotação da chave da raiz do DNS, que deverá ser concretizada a 11 de outubro, prosseguindo os trabalhos iniciados no ano passado.

Toda a comunidade concorda, mesmo tendo em conta que, apesar dos dados iniciais, não há dados concretos sobre o facto do RollOver poder falhar ou gerar problemas.

SAIBA MAIS EM:

Relatório CENTR: https://centr.org/library/library/external-event/centr-report-on-icann61.html
Comunicado do GAC: https://gac.icann.org/contentMigrated/icann61-gac-communique



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

Produção: maio 2018
Grafismo: dns.pt