ICANN 59
POLICY FORUM

JOHANNESBURG
26–29 June 2017

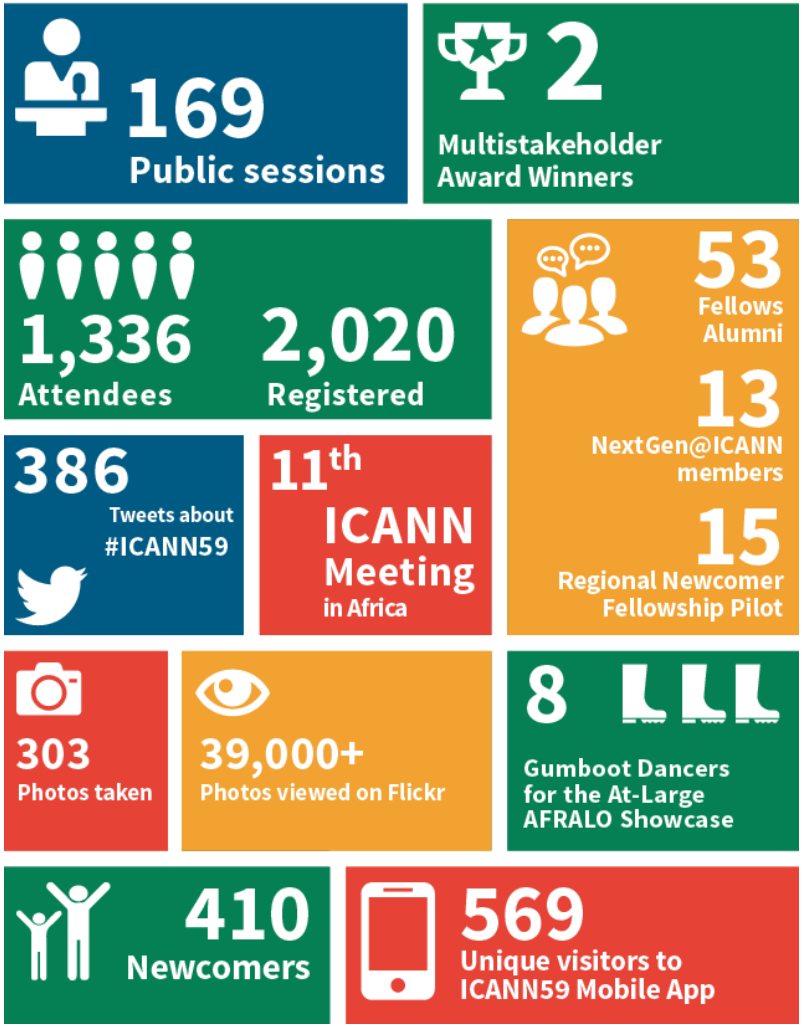
RELATÓRIO DNS.PT

ÍNDICE

INTRODUÇÃO

A edição 59 da ICANN decorreu em Joanesburgo, África do Sul, entre os dias 26 e 29 de junho de 2017.Tratou-se da reunião intercalar do ano, mais reduzida e mais direcionada ao desenvolvimento e discussão de políticas pela comunidade, em muito concentrada nos trabalhos conduzidos por grupos de trabalho como o ccNSO, o GNSO, o GAC, entre outros. Nesta policy meeting, para além das matérias de natureza técnica às quais estamos particularmente atentos, destacamos três assuntos sobre os quais deixamos algumas notas e que esperamos ser úteis e de interesse para a nossa comunidade nacional: Utilização de nomes geográficos e territórios como domínios de topo; Registo no segundo nível de 2 caracteres coincidentes com códigos de países e GDPR.

ICANN 59 EM NÚMEROS



UTILIZAÇÃO DE NOMES GEOGRÁFICOS E TERRITÓRIOS COMO DOMÍNIOS DE TOPO

Desde 2005 que, especialmente o GAC tem vindo a defender que a ICANN deve impedir que os nomes de países e territórios constem na esfera dos novos gTLD´s, como domínios de topo. Segundo o GAC, e em termos macro, deverá proteger-se os nomes de âmbito geográfico, tendo em conta aspetos como a autodeterminação dos povos, a sua soberania, a sua cultura e individualidade, e mais ainda, porque o utilizador final não deve ser induzido num pressuposto errado, consultando um site cujo conteúdo deveria estar associado a algum país ou território e tal simplesmente não verificar-se. A linha hoje defendida pelo GAC, vai ao encontro dos princípios defendidos na ICANN Lisboa, no já longínquo dia 28 de março de 2007, ou seja, que os novos gTLDs devem respeitar os nomes que contenham um importante significado a nível geográfico. Ou seja, devem ser protegidos os códigos de 2 letras; as 274 combinações de 3 letras que resultam do ISO 3166; os nomes dos países e respetivas traduções e os nomes das capitais e principais cidades mundiais.

O CCWG country and territory names, criado em março de 2014, ainda não conseguiu encontrar consensos, com uma única exceção: a proibição absoluta de utilização dos códigos de 2 letras. Ora, decididamente, também aqui a doutrina diverge. No GNSO[1] algumas vozes chegaram mesmo a alvitrar a possibilidade de registo de códigos de duas letras como foi o caso, por exemplo,

[1] *https://gnso.icann.org/en/*

do .VW, de qualquer forma é amplamente defendido que os códigos de 3 letras, mesmo se constantes no ISO 3166 alpha -3, devem ficar disponíveis assim como os nomes dos países. Defendem ainda que os titulares de marcas têm pleno direito sobre o respetivo elemento nominativo ainda que este coincida com uma designação geográfica[2]. Do lado oposto temos o GAC[3] que defende que as regras hoje aplicáveis aos nomes geográficos não protegem suficientemente países e territórios devendo ser inclusivamente extensíveis a lugares, rios, montanhas, etc.

Ora, também numa ótica de interesse público, o GAC defende que a representação de duas letras de nomes de países e territórios no padrão ISO231-1 alpha2, reservada aos ccTLDs, deve ser mantida. Mais, alega o GAC que o Board da ICANN deve tomar uma decisão perentória, no sentido de não permitir que qualquer abreviatura de nomes de países ou de territórios seja delegada aos novos gTLD´s[4], na medida em que são uma exteriorização do espaço geográfico e como tal, devem somente ser administrados por ccTLD´s. No entanto, caso a ICANN adote uma posição contrária, o GAC argumenta que deverá ser imposta a exigência aos novos gTLD´s, de obterem uma declaração de autorização do Governo do território em causa ou de autoridade pública competente.

Neste sentido, é relembrada a proibição de registo de novos gTLD´s relativos a nomes de países e territórios prevista no New gTLD Applicant Guidebook[5], em junho de 2012, no ponto 2.2.1.4.1, especificamente, os códigos alfa-3 listados na ISO 3166-1, os nomes de país ou territórios listados na ISO 3166-1, ou uma tradução em qualquer língua do nome desse país ou território, ou os códigos que constam da Lista de Nomes de Países do referido Guia, que dizem respeito aos códigos que não refletem o nome comum do país.

2 *Veja-se o caso do .amazon*

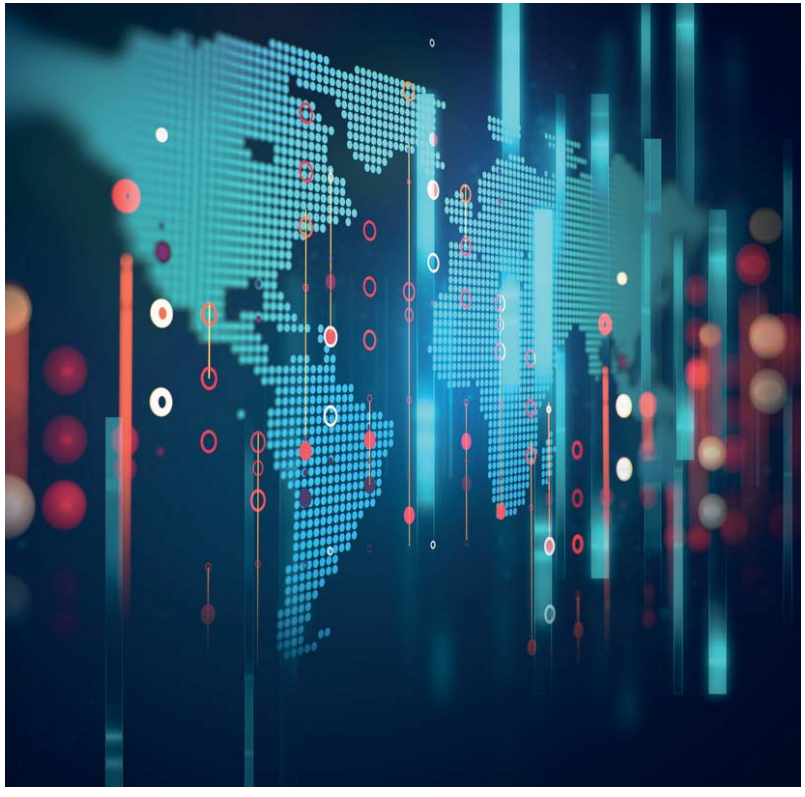
3 *https://gacweb.icann.org/*

4 *Aquando do lançamento dos novos gTLD's merecem-nos nota o caso do .IOT que não foi aceite já que é o acrónimo de Indian Ocean Territory, e do próprio .IDN que foi recusado por se tratar do código de 3 letras da Indonésia.*

5 *https://newgtlds.icann.org/en/applicants/agb*

Mais, de acordo com o estatuído no ponto 2.2.1.4.2, do referido Guia a permissão de delegação de certos nomes geográficos aos gTLD´s, implica, concretamente, a obrigação de entrega de documentação de suporte que titule o direito. Ainda, deve ser apresentado o acordo estabelecido com o governo a que esta decisão afeta, ou com autoridade pública com competência para analisar a questão. Do mesmo modo que os nomes semelhantes a países e territórios que possam causar confusão ao consumidor, deverão igualmente ter a respetiva permissão expressa por parte do Governo eventualmente afetado por essa decisão.

A este propósito foram discutidas ideias como a criação de uma lista de nomes geográficos concretos de relevo para aditar já à lista espelhada no Guia do Candidato dos novos gTLD´s. De modo a proteger os Registries, defende o GAC que nos casos em que há permissão do Governo, para o registo de um gTLD, com semelhanças e repercussões num ccTLD, deverá estabelecer-se uma cláusula no Contrato de Registo entre a ICANN e a entidade responsável pelo novo gTLD, para havendo disputa entre um Registry responsável por um ccTLD e um novo gTLD, a ICANN estar vinculada a cumprir a decisão tomada na jurisdição do território em causa. Consequentemente, propõe o GAC a existência de mecanismos adequados para a resolução de litígios referentes a estas questões. O CENTR já manifestou de forma pública a sua posição, de resto sufragada pelos seus associados. Assim, é defendido que os mecanismos e salvaguardas fixadas no New gTLD Applicant Guidebook, são suficientes e traduzem um equilíbrio entre os interesses em causa, qualquer alteração a efetuar neste âmbito deve estar condicionada à vontade e participação de toda a comunidade interessada. Neste momento esta é ainda como que, digamos, uma "não questão" na medida em que a ICANN ainda não anunciou data para as novas candidaturas a registo de novos gTLD's, mas esta vai chegar e questões como esta terão de estar fechadas e, se possível, deverão encerrar o maior consenso possível da comunidade.



REGISTO NO SEGUNDO NÍVEL DE 2 CARACTERES COINCIDENTES COM CÓDIGOS DE PAÍSES

Também esta matéria é recorrente e identificada como uma das mais criticas e controversas no panorama da ICANN. Dispensa, pois, o habitual enquadramento sob pena de redundância de informação. A questão agudizou-se com a decisão do board do final do ano de 2016, nos termos da qual os novos gTLD's podem aceitar o registo de domínios coincidentes com códigos de 2[6] letras de países desde que, de alguma forma, implementem medidas tendentes a evitar confusão ou erro no consumidor final. Referimo-nos em concreto à existência de politicas próprias e bem definidas que contenham medidas para dirimir e averiguar conflitos com países ou territórios e a possibilidade destes últimos terem como que um direito de preferência, vigente por um prazo não inferior a 30 dias, para protegerem o registo do respetivo código. Refira-se que sobretudo os designados dotBrands[7] gTLD'S estão a utilizar amplamente os códigos de países como domínios de segundo nível Curiosamente decorre daqui uma questão paralela, os países que têm manifestado maior interesse em proteger o TLD são aqueles que ao longo do tempo têm defendido um maior peso do Estado na gestão do respetivo ccTLD. Inclusivamente, uma das hipóteses que chegou a estar em discussão, ainda que informalmente, foi a possibilidade dos governos terem direito de veto no que à possibilidade de utilização do ccTLD por gTLD's diz respeito. Isto com base na ideia do ccTLD se tratar de um suposto "bem ou ativo público". Essa possibilidade foi de imediato afastada, maioritariamente pelos defensores do modelo multistakeholder invocando que no âmbito dos processos associados à governação da Internet nenhum voto vale mais do que outro. De qualquer forma, a própria decisão da ICANN terá ido à revelia da vontade do GAC e do próprio ccNSO[8] que nunca se pronunciou em sentido favorável a esta possibilidade. Ou seja, se os países representados no GAC não são unanimes no sentido de considerarem dever proteger o respetivo código ISO 3166, já não é assim quando é analisado o processo que conduziu a esta tomada de decisão da ICANN. De novo, o processo decisório e a eficácia dos mecanismos de influência na decisão do board, ficaram em causa, do nosso ponto de vista com toda a propriedade.

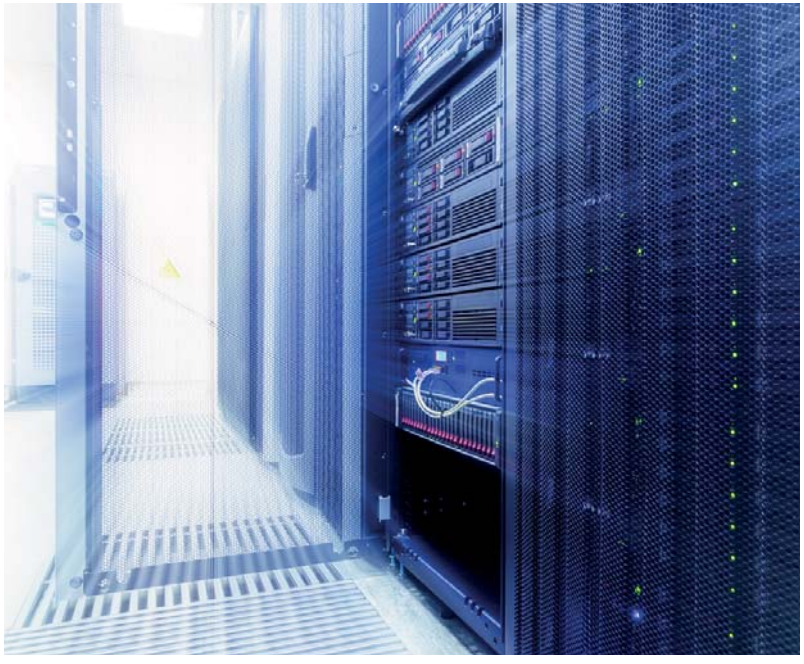
6 *ISO 3166-1 alpha*

7 *Domínios genéricos de topo correspondentes a marcas, por exemplo: Deloitte, Canon, Apple, BBC, Gucci, Sony, etc. Constituem 34% das 1930 candidaturas que foram submetidas à ICANN aquando do lançamento do programa. Atualmente estão já ativos cerca de 540 dotBrand gTLD's, com um total não superior a 6900 registos.*

8 *Isto não obstante países com o UK, a Bélgica ou a Alemanha – membros efetivos do ccNSO – defenderem abertamente que nada têm a por à utilização do respetivo código de 2 letras como domínios de 2.º nível.*

GDPR

Não fosse este o assunto do momento e esta edição da ICANN, onde supostamente a discussão estaria mais focada num suposto core técnico, não estaria completa. O enfoque das duas sessões GDPR[9] centrou-se numa dupla de pontos essenciais: saber até que ponto os países fora da União Europeia estão abrangidos pela esfera de aplicação do novo Regulamento de Proteção de Dados e, qual o impacto do articulado do diploma naquilo que é hoje o WHOIS[10].



A ICANN não ficou alheia à relevância destas duas questões e, de novo, ao impacto destas nas obrigações e responsabilidades vertidas nas centenas de contratos já assinados com os registries dos gTLD's. Note-se que na AOC[11] se previa expressamente que os registries deviam, passamos a transcrever: "(...) *implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information* (...)". Ou seja, a ICANN tem já hoje implementadas medias conducentes a mitigar eventuais conflitos que resultem de violações de leis nacionais em matéria de proteção de dados, quando em causa está a obrigação de disponibilização de dados pessoais, sobretudo de registrants, via WHOIS. Nesse sentido, e tentando fazer face a eventuais conflitos, foi criado um procedimento formal que deve seguir os seguintes trâmites:

O processo tem inicio com a notificação pelo registry à ICANN de que por determinada imposição decorrente de lei nacional aplicável não poderá cumprir com as disposições constantes no seu contrato com a ICANN, em relação à recolha e/ou publicação de dados, através do WHOIS. Caso o Registry opte por não enviar a referida notificação à ICANN, poderá em alternativa, apresentar à ICANN uma declaração escrita da autoridade nacional competente na matéria, em Portugal a CNPD, invocando a eventual violação da lei aplicável. Após a receção e revisão da notificação, a ICANN consultará o Registry sobre o processo e caso seja necessário, poderá consultar as autoridades nacionais ou outros requerentes. Trata-se de uma fase de consulta onde é tentada resolução do litígio pendente de modo a que o Registry

9 *EU General Data Protection Regulation - http://www.eugdpr.org/.*

10 *https://whois.icann.org/en/about-whois*

11 *ICANN's Affirmation of Commitments https://www.icann.org/resources/pages/affirmation-of-commitments-2009-09-30-pt*

cumpra as suas obrigações contratuais com a ICANN, no que diz respeito ao WHOIS. O processo, ao qual entretanto é associado um relatório completo e uma proposta de resolução, segue então para deliberação do board da ICANN. Tendo em conta o impacto da decisão final no que respeita ao funcionamento e possíveis alterações às regras aplicáveis ao WHOIS, o board poderá solicitar informações adicionais ao Registry ou a terceiros interessados; abrir um período para comentários públicos; ou mesmo enviar o processo para revisão e comentários do GNSO. A decisão final é comunicada ao registry e divulgada no site da ICANN. De qualquer forma, o compromisso é sempre o de encontrar uma solução de consenso entre os compromissos contratuais assumidos entre o registry e a ICANN e a lei aplicável em matéria de proteção de dados.

Nas sessões sobre o GDPR, para além do necessário enquadramento geral sobre o alcance do diploma, que aqui não será objeto de análise, foi dado especial enfoque ao respetivo impacto na indústria dos domínios que se perspetiva. Primeiro, haverá aproximadamente 60 elementos que são recolhidos no processo de registo ou manutenção de um domínio e que podem constituir-se como dados pessoais, referimo-nos em concreto a nomes, moradas, emails, telefones, endereços IP, determinados nomes de domínio[12], etc. Referimo-nos ainda a várias possibilidades ao nível do tratamento e processamento de dados que vão desde o registo online, ao escrow de informação, publicação no WHOIS, etc. Todo este manancial de informação hoje recolhido pelos registries e registrars deve ser avaliado por forma determinar o que é efetivamente necessário para gestão e funcionamento do negócio, num principio que agora vai imperar de minimização na recolha e tratamento de dados pessoais e possível pseudonimização.

A questão dos prazos de conservação e a acessibilidade aos dados, deve também ser especialmente acautelada. As regras para obtenção do consentimento dos titulares dos dados, passando a ser muito mais exigentes, vão implicar criar mecanismos de obtenção de um consentimento claro, expresso e obtido especificamente para o tratamento de dados a que respeita. Aqui, a revisão dos contratos passados por forma a que passem também eles a cumprir o previsto no GDPR será fundamental.

Importante será também enquadrar o conceito de registry e registrar nas figuras de responsáveis pelo tratamento dos dados (controllers) e dos subcontratantes (processors).

12 *Por exemplo: luisgueifao.pt*

Note-se que o regulamento, ao invés do que acontecia ao abrigo da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, prevê que as entidades em regime de subcontratação, designadas de "subcontratantes", passem a ter praticamente as mesmas obrigações que os responsáveis pelos tratamentos. Acresce que o GDPR veio elencar os termos a que devem obedecer os contratos de subcontratação, ou seja, registries e registrars têm de reavaliar a relação formal que os tem vindo a nortear. A título de exemplo, sempre que haja subcontratação, cabe ao subcontratante verificar se detém as autorizações respetivas dos responsáveis pelo tratamento, caso contrário, deve obtê-las, preferencialmente até 25 de maio do próximo ano.

Neste momento a ICANN está a trabalhar na designada Next-Generation gTLD Registration Directory Services, RDS, que substituirá o WHOIS como hoje o conhecemos. O compromisso será integrar neste novo sistema grande parte dos princípios inerentes ao GDPR, de resto, este pressuposto foi publicamente defendido pelo GAC que alertou para a importância deste esforço por parte do board da ICANN. Vamos aguardar, certos porém que o assunto está a ser atentamente acompanhado neste fórum.

ICANN | 59 • TECH DAY

COMBATE AO PHISHING NA CHINA

Ning Kong do CNNIC expôs alguns dados sobre ataques de Phishing na China e os esforços que têm sido desenvolvidos para combater este problema. O CNNIC é o Registry responsável pela gestão do ccTLD .cn da China desde 1997, e pelos ccTLD's com caracteres especiais (IDN) .xn--fiqs8s em chinês simplificado e o .xn--fiqz9s em chinês tradicional desde 2010.

O .cn é um domínio de topo com grande popularidade, com mais de 21 Milhões domínios registados, ficando apenas abaixo do .com. Esta popularidade é o resultado do crescimento continuou de utilizadores da internet na China, incentivos no preço e uma política de registo de domínios favorável ao crescimento.

Figura 1- Total de ataques de Phishing na China

(fonte : http://schd.ws/hosted_files/icann59johannesburg2017/ca/8%20CNNIC%20Ning%20Kong%20-%20Improving%20Domain%20Names%20Utilization.pdf, pág.3)

Nos últimos 6 anos o número de ataques com esta tipologia na China cresceu 318%, mas foi sobretudo em 2016 que este crescimento foi mais acentuado chegando a 147,211 ataques, um aumento de 151% face ao ano anterior.

Os sectores mais afetados por ataques de Phishing na China, à semelhança dos restantes países, são as plataformas de pagamentos transacionais, as instituições financeiras, as empresas de comunicações eletrónicas e as plataformas de E-commerce. Organizações como a *TaoBao* similar à Amazon, o *Bank of China* e a *China Mobile* estão frequentemente envolvidas em ataques de Phishing.

Em relação os domínios de topo utilizados nos ataques Phishing na China, o .com é o preferido em 64,24% dos casos, o .cc, ccTLD das Ilhas Cocos (Keeling) em 14,95%, e o .pw ccLTD da República de Palau em 6,09%.

Apesar da grande popularidade do .cn, este apenas é utilizado em 1,39% dos ataques de Phishing. O CNNIC acredita que a reduzida utilização do .cn em ataques de Phishing resulta da implementação duma politica de verificação muito estrita, que correlaciona os dados de identificação de cidadãos nacionais e estrageiros, nomes de domínios, dados das redes sociais, e os conteúdos na Internet. Esta politica permite a identificação rápida dos responsáveis pelos conteúdos online, um ponto chave que permite a eliminação de mais de metade dos ataques de Phishing, no período entre 1 a 3 dias, porém muitos ataques ainda tem uma duração superior a 10 dias.

Para combater o problema de Phishing, o CNNIC criou o *Anti-Phishing Alliance of China* (APAC) em 2008, uma organização sem fins lucrativos não governamental, responsável pela coordenação e realização de iniciativas de combate ao Phishing. No final de 2016 esta organização era composta por 523 membros, agências financeiras, empresas de e-commerce, Registries, Registrars e organizações de cibersegurança, em suma, os sectores mais envolvidos em ataques de Phishing.

A APAC recebe com regularidade relatórios de atividade de Phishing do público e dos seus membros, realiza ações de pesquisa e análise, e colabora com organizações internacionais como o APWG (http://www.antiphishing.org/). A informação com origem no público é reconhecida e validada por uma organização técnica independente, antes de procederem ao tratamento das mesmas.

Na fase de eliminação dos ataques Phishing pela APAC há três casos de uso.

- Se o domínio está registado na China,
  - e o site é totalmente falso, então o domínio é removido da internet, pelo Registry/Registrar;
  - e o site é real, mas tem uma ou duas páginas de Phishing, então o Registry/Registrar solicita a remoção desses conteúdos;
- Se o domínio está registado num país estrangeiro, as empresas de cibersegurança emitem alertas e os browsers exibem um aviso de Phishing no acesso ao site;

2016 foi o ano de maior atividade da APAC no combate Phishing, dos 147,211 ataques já referidos, foram identificados e processados um total de 107,303 casos Phishing. Acumulativamente a APAC já processou um total de 385,996 ataques de Phishing desde da sua criação.

Após a criação da APAC, o CNNIC continuou a apostar no combate ao Phishing com vários contributos importantes, nomeadamente o desenvolvimento do sistema "Proactive Phishing Detection System", baseado em conceitos de *Big* Data e *machine learning*. A publicação de 10 artigos académicos e o registo de 10 patentes de soluções Anti-Phishing. Por último, o CCNIC e a APAC publicam regularmente relatórios sobre a evolução de Phishing na China.

NOVO SISTEMA DE INFORMAÇÃO DE REGISTO DO CCTLD .RS (SERVIA)

Danko Jevtović, CEO do RNIDS, o registry responsável pela gestão dos ccTLDs .rs e .срб em cirílico, da Sérvia, apresentou o seu novo sistema de registo. O RNIDS foi criado em 2007 com a missão de gerir o ccTLD .rs, sucessor do antigo .yu ccTLD da extinta lugoslávia.

O RNIDS sentiu necessidade de implementar um novo sistema de informação, porque o anterior já não se adequava às necessidades do .rs. O antigo sistema era uma herança do .yu, baseado em software livre académico, sem suporte para Registrars, com *web services* desenvolvidos à medida das necessidades e não compatíveis com EPP, sem suporte para DNSSEC, com desenvolvimentos feitos à medida das necessidades imediatas e com possíveis falhas de segurança desconhecidas. Em síntese, o antigo sistema tornou-se demasiado desajustado e complexo.

O RNIDS identificou como requisitos do novo sistema informação: uma solução moderna de software modular, no formato web e responsive, com uma interface standard de EPP que permitisse a comunicação normalizada com os Registrars, com procedimentos simplificados e orientada por princípios de Security by design (OWASP[13]). Por último, a solução tinha de ter um preço acessível, porque o .rs é um ccTLD de pequena dimensão, menos de 100,000 domínios.

13 *https://www.owasp.org/index.php/Security_by_Design_Principles*

O RNIDS ponderou então as várias soluções, manter o código anterior não era possível, soluções de serviços de Registry já desenvolvidas não era uma opção devido ao seu preço elevado, o software "Fred" desenvolvido pelo .CZ teria de ser modificado e o .RS não tinha recursos técnicos para assegura esses trabalhos e por último colocar as operações do Registry em outsource estava fora de questão.

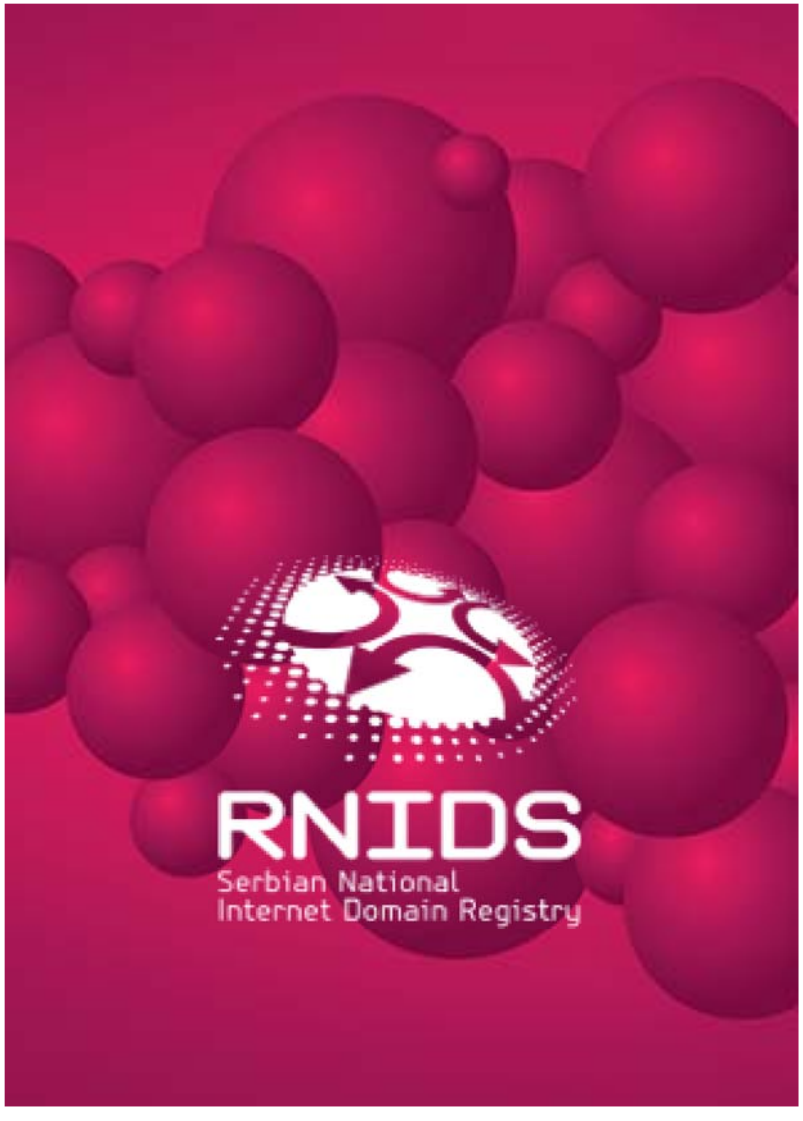
Em 2011 o RNIDS decidiu dividir o projeto em duas componentes, a primeira composta pela especificação de requisitos e a segunda pela criação do software. Em 2013 a primeira parte foi entregue à Escola de Engenharia Eletrónica de Belgrado, e um ano depois estava concluída e aceite. Para a segunda parte, o RNIDS lançou em 2014 um concurso internacional, no entanto estes trabalhos foram entregues a uma empresa local de pequena dimensão que já trabalhava com o Registry. Esta empresa produziu o software durante 2015, um ano depois o RNIDS adquiriu e implementou uma nova infraestrutura de Hardware.

O sistema de informação resultante é totalmente configurável, com uma implementação standard de EPP, suporta o registo de domínios IDN, está preparado para DNSSEC, tem acessos seguros para Registrars com *Two Factor Authentication* (2FA) e *One Time Password* (OTP), tem vários mecanismos de segurança opcionais para Registrars, tem demonstrado um bom desempenho e é seguro, por último o sistema é multilíngue.

A migração de sistemas de informação do RNIDS ocorreu a 26 de junho de 2016 durante 5 horas. Não ocorreram problemas de maior e está a funcionar desde de então.

As lições retiradas pelo RNIDS deste processo, são: os princípios de *Security by design (OWASP)* foram muito importantes, todo o código e procedimentos foram testados minuciosamente, apesar do EPP ser um standard foi necessário criar uma ferramenta de testes EPP, foi um processo muito longo e oneroso para o Registry, e o sucesso foi garantido devido a um planeamento antecipado.

Futuramente o RNIDS planeia implementar o registo de domínios IDN's no .rs, DNSSEC e algumas extensões de marketing. Por fim, o RNIDS está disponível para parcerias de outros Registries que decidam implementar e explorar o novo sistema de informação.



GAC SESSION ON THE KSK ROLLOVER

No último dia desta edição da ICANN, David Conrad CTO da ICANN realizou junto do GAC, uma sessão sobre o processo de rollover da chave KSK da root.

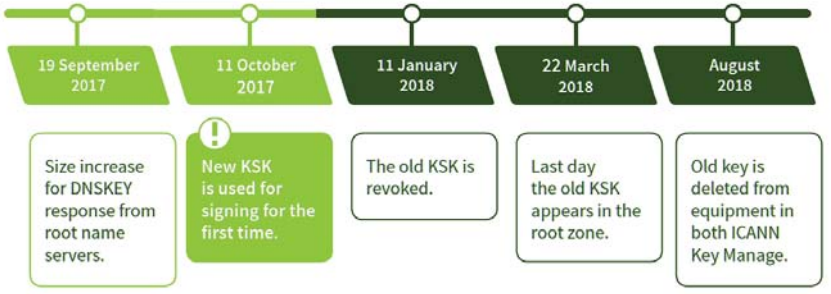
A chave KSK pública da root denominada por Trust Anchor, é o topo hierárquico da chain of trust, uma estrutura utilizada para validar domínios com DNSSEC. Todos os servidores Resolvers que fazem validação DNSSEC tem de ter uma cópia desta chave para processar a validação DNSSEC.

As diretivas de gestão DNSSEC da chave KSK da root, estabelecidas pela ICANN no documento "*DNSSEC Practice Statement for the Root Zone KSK Operator*" ou DPS[14] definem, passamos a transcrever: "(...) Each RZ KSK will be scheduled to be rolled over through a key ceremony as required, or after 5 years of operation. (...)". Como a chave atual foi gerada em 2010, tornou-se imperativo proceder à sua substituição.

14 *https://www.iana.org/dnssec/icann-dps.txt*

A ICANN desenvolveu várias iniciativas nesta matéria desde 2012, donde se destacam as duas últimas, as recomendações do grupo SSAC no estudo SAC-063 (https://www.icann.org/en/system/files/files/sac-063-en.pdf) em 2013, e por último o relatório do grupo de trabalho "KSK Roll Design Team" constituído por especialistas em DNS/internet de vários países em 2016. Estes trabalhos foram precursores do plano operacional (https://www.icann.org/resources/pages/ksk-rollover/#operational-plans) do processo de rollover da chave KSK, em curso.

Figura 2- Principais etapas do processo de rollover da KSK da root



(https://ccnso.icann.org/meetings/johannesburg59/presentation-ksk-rollover-26jun17-en.pdf Pág.4)

O ponto crítico deste processo irá ocorrer no próximo dia 11 de outubro, quando a nova chave KSK começar a ser utilizada na assinatura da zona root. Note-se, contudo, que o processo de rollover da chave KSK decorre por fases ao longo de vários meses, sendo possível testar e corrigir o comportamento dos sistemas antecipadamente.

O ponto crítico deste processo irá ocorrer no próximo dia 11 de outubro, quando a nova chave KSK começar a ser utilizada na assinatura da zona root. Note-se, contudo, que o processo de rollover da chave KSK decorre por fases ao longo de vários meses, sendo possível testar e corrigir o comportamento dos sistemas antecipadamente.

Todas as entidades que disponibilizam servidores Resolvers com validação DNSSEC, têm de garantir que os seus sistemas irão reconhecer a nova chave KSK. A maioria dos servidores deverá faze-lo de forma automática (RFC 5011 "Automated Updates of DNS Security"), se o software DNS que usam estiver atualizado. Os restantes servidores que não irão reconhecer a nova chave de forma automática, tem de ser configurados manualmente.

No dia 11 de outubro e seguintes, os servidores que não reconheçam a nova chave KSK irão falhar a validação DNSSEC e os utilizadores ficarão impossibilitados de aceder aos serviços/conteúdos internet pretendidos.

Para se ter uma ideia da dimensão do universo de sistemas potencialmente afetados, estima-se que existam aproximadamente 100 milhões Servidores Resolvers, dos quais 25% fazem validação DNSSEC.

A ICANN disponibiliza uma plataforma de testes[15] que pode ser utilizada para verificar se os sistemas de Resolver estão preparados para o rollover da chave KSK da root.

O Rollover da chave KSK da root tem sido bastante divulgada nos últimos dois anos, nomeadamente em fóruns técnicos enquanto decorria o trabalho da equipa "KSK Roll Design Team". Nos últimos meses a ICANN tem procurado todos os meios e fóruns possíveis para alertar a comunidade, num último esforço para evitar problemas decorrentes do processo de rollover em curso.

A par destes desenvolvimentos e por iniciativa própria, o DNS.PT tem vindo a promover nos últimos meses, encontros com os principais operadores de comunicações nacionais, para sensibilizar estas entidades para o processo de rollover da chave KSK da root e discutir o nível de preparação dos sistemas de resolução DNS nacionais. Os resultados destes encontros têm sido bastante positivos, a principal evidência é o envolvimento e o interesse demonstrado por estas entidades.

15 *https://automated-ksk-test.research.icann.org/*

No decorrer da ICANN 59 realizou-se mais um Workshop DNSSEC, uma iniciativa do SSAC (https://www.icann.org/groups/ssac) com apoio do programa Deploy360 da ISOC (https://www.internetsociety.org/). Mais uma vez reuniram-se vários membros da comunidade técnica envolvidos no desenvolvimento e implementação de DNSSEC, responsáveis de ccTLD's e diversas organizações da industria DNS.

Como é habitual, foi apresentado o estado atual de implementação DNSSEC. Quase metade dos ccTLD's já se encontram assinados com DNSSEC, sendo que a América do Norte e a Europa são as regiões com as maiores taxas de implementação, na vertente oposta, nas regiões de Africa, Ásia Pacifico e América Latina ainda há vários ccTLD's sem DNSSEC. O .lr da Libéria e o .sa da Arabia Saudita são os últimos ccTLD's com DNSSEC, assinados em abril e junho respetivamente.

Em relação à validação de consultas DNS com DNSSEC, a média global situa-se nos 14%. No continente africano este valor é de 15,09%, mas note-se que, quase 30% do tráfego DNS validado com DNSSEC em Africa é assegurado pelo serviço *Google Public DNS* (https://developers.google.com/speed/public-dns/), o que pode significar uma menor preparação dos operadores de comunicações regionais para DNSSEC.

O relatório "*State of DNSSEC Deployment 2016*" (https://www.internetsociety.org/doc/state-dnssec-deployment-2016) elaborado pelo ISOC, reúne um conjunto de dados essencial para uma análise completa e detalha da implementação de DNSSEC na internet.

Na sessão sobre os desafios da implementação de DNSSEC moderada por Mark Elkins, foram referidos uma vez mais os principais obstáculos à adoção de DNSSEC em Africa, nomeadamente a falta de recursos com conhecimentos em DNS/DNSSEC, a falta de interesse da comunidade local, desconhecimento do risco de não ter DNSSEC e por último, os registries não estão preparados para DNSSEC.

A iniciativa "Africa DNSSEC roadshow" (https://www.icann.org/news/blog/dnssec-for-securing-cctlds-in-africa) criada pela ICANN em 2013, tendo vindo a apoiar os ccTLD's africanos, nomeadamente através da realização de workshops DNSSEC em vários países.

A terceira e ultima parte dos Workshop DNSSEC durante a ICANN 59 consistiu da apresentação e discussão de temas relacionadas com a evolução do DNSSEC.

Tipicamente a titularidade e gestão de domínios baseiam-se no modelo Registry, Registrar e Registrant, porém este modelo nem sempre corresponde à realidade. Nalguns casos há entidades adicionais envolvidas na gestão de domínios, como Revendedores DNS e operadores DNS. Contudo, estas entidades não são reconhecidas pelo ICANN, o que coloca grandes dificuldades nas funções que as mesmas despenham, nomeadamente a operação de registos DNS e DNSSEC. Para resolver o problema a comunidade técnica desenvolveu um conjunto de soluções como CDS/CDNSKEY "RFC 8078 - *Managing DS Records from the Parent via* CDS/CDNSKEY" e CSYNC "RFC 7477 - *Child-to-Parent Synchronization in DNS*", que automatizam a interação para troca de dados de registos DNS entre as entidades que participam na gestão dos domínios. Contudo, não existe por parte da ICANN um reconhecimento do problema e por consequência da diretiva a adotar.

O objetivo principal desta sessão era identificar os mecanismos da ICANN para gerar discussão e resultados em torno dos problemas e soluções expostos.

Patrik Faltstrom, sugeriu um conjunto de passos que podem levar ao inicio da discussão do problema na ICANN, tais como identificar uma solução que realmente funcione independentemente da comunicação dos operadores DNS ser feita com os Registries ou com os Registrars, e o EPP deverá ser adaptado para contemplar uma notificação adicional para funções autónomas.

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

Produção: julho 2017
Grafismo: dns.pt