ICANN | GAC
Governmental Advisory Committee

ICANN 68
VIRTUAL POLICY FORUM
22–25 June 2020

Mitigação de abusos do DNS

Sessões 2 e 8

Índice

Objetivos da sessão

O GAC discutirá os acontecimentos recentes relacionados a Abusos do DNS, particularmente no contexto da crise da COVID-19, referentes a uma sessão de Plenária entre Comunidades planejada sobre esse tópico durante o ICANN68. Essa sessão também será uma oportunidade de revisar e debater os acontecimentos relevantes para a prevenção e a mitigação de Abusos do DNS e Ameaças à Segurança.

Histórico

As atividades maliciosas na Internet ameaçam e afetam os registrantes de nomes de domínio e usuários finais aproveitando as vulnerabilidades em todos os aspectos dos ecossistemas da Internet e do DNS (protocolos, sistemas de computadores, transações pessoais e comerciais, processos de registro de domínios etc.). Essas atividades inescrupulosas podem ameaçar a segurança, a estabilidade e a resiliência das infraestruturas do DNS e do DNS como um todo.

Essas ameaças e atividades maliciosas geralmente são chamadas de "Abuso do DNS" na Comunidade da ICANN. Em geral, entende-se que Abuso do DNS refere-se a atividades inteiras ou parte delas, como ataques de DDoS (Distributed Denial of Service, Negação de Serviço Distribuída), spam, phishing, malware, botnets e a distribuição de materiais ilegais. Embora todos concordem que os abusos do DNS sejam um problema que precisa ser resolvido, existem opiniões diferentes sobre a quem atribuir essa responsabilidade. Os Registros e os Registradores, em particular, estão preocupados que seja solicitado que eles façam mais, já que isso afeta o modelo de negócios e o escopo deles.

Como parte desta discussão, é importante observar que até mesmo a definição exata de "Abuso do DNS" é um assunto para debate[1].

Ainda assim, a discussão progrediu nos últimos anos. Este é um resumo dos trabalhos realizados anteriormente pela Comunidade da ICANN para solucionar o Abuso do DNS, e alguns deles contaram com a participação do GAC:

- A **GNSO (Generic Names Supporting Organisation, Organização de Apoio a Nomes Genéricos)** da ICANN organizou um Grupo de Trabalho sobre Políticas de Abuso de Inscrições em 2008. Ele identificou um conjunto de assuntos específicos, mas não produziu resultados de políticas e também não realizou uma discussão subsequente sobre práticas recomendadas não vinculativas para Registros e Registradores (inclusive workshops durante o ICANN41 e o ICANN42).
- **Como parte do Programa de Novos gTLDs**, a adoção pela Organização ICANN de uma série de novos requisitos[2] de acordo com seu memorando sobre Mitigação de Condutas Maliciosas (3 de outubro de 2009). Relatório da ICANN sobre as Proteções do Programa de Novos gTLDs (18 de julho de 2016) avaliou sua eficiência em preparação para a Relatório de CCT (Competition, Consumer Trust and Consumer Choice; Concorrência, Confiança e Escolha do Consumidor), definida pelo Estatuto, que apresentou suas recomendações em 8 de setembro de 2018.

[1] Conforme evidenciado na discussão sobre Abusos do DNS e Proteções do Consumidor durante a Cúpula da GDD (7 a 8 de maio de 2019).

[2] Investigar os operadores de registro, exigir um plano demonstrado para a implementação de DNSSEC, proibir o uso de caracteres curinga, remover registros glue órfãos quando uma entrada no servidor de nomes for removida da zona, exigir a manutenção dos registros de WHOIS thick, a centralização do acesso de arquivos de zona, exigir procedimentos e contatos de abuso no nível do registro documentados.

- Antes da criação do PSWG (Public Safety Working Group, Grupo de Trabalho sobre Segurança Pública) do GAC, os **representantes de LEAs (Law Enforcement Agencies, Agências Legais Fiscalizadoras)** tiveram uma posição de liderança na negociação do Contrato de Credenciamento de Registradores de 2013[3], bem como na elaboração do Conselho do GAC relacionado a Ameaças à Segurança, que resultou em novas disposições no Contrato Básico de Novos gTLDs que descrevia as responsabilidades dos registros. Essas disposições foram posteriormente complementadas por uma Estrutura para Operadores de Registros Responderem a Ameaças à Segurança (20 de outubro de 2017) não vinculativa e acordada entre a **Organização ICANN, Registros e o PSWG do GAC**.

- O **SSAC (Security and Stability Advisory Committee, Comitê Consultivo de Segurança e Estabilidade)** emitiu recomendações para a Comunidade da ICANN, em particular no SAC038: Ponto de Contato de Registradores para Abusos (26 de fevereiro de 2009) e no SAC040:Medidas para Proteger os Serviços de Registro de Domínios contra a Exploração ou o Mau Uso (19 de agosto de 2009).

- A **Organização ICANN**, pela **equipe de SSR (Security and Stability Review, Revisão de Segurança e Estabilidade)**, treina regularmente as comunidades de segurança pública e ajuda a responder a incidentes cibernéticos de grande escala, inclusive por meio do processo de ERSR (Expedited Registry Security Request, Solicitação Expressa de Segurança no Registro). Mais recentemente, o **Escritório do CTO** desenvolveu o DAAR (Domain Abuse Activity Reporting, Geração de Relatórios de Atividade de Abuso de Domínios) da ICANN e produz Relatórios de Abusos mensais. Essa ferramenta tem sido apoiada veementemente pelo GAC e por várias Equipes de Revisão Específica como uma forma para criar transparência e identificar as causas dos problemas, que podem, assim, ser solucionados por meio da conformidade ou, quando necessário, uma nova política.

Questões

As iniciativas anteriores ainda não resultaram em uma redução efetiva de abusos do DNS. Pelo contrário, está mais claro que ainda há muito a ser feito. Apesar da atenção da Comunidade da ICANN e as práticas recomendadas existentes do setor para mitigar Abusos do DNS, algumas iniciativas de participação da comunidade lideradas pelo GAC, bem como a Análise Estatística sobre Abusos do DNS em gTLDs da Revisão de CCT (9 de agosto de 2017), destacaram tendências persistentes de abuso, práticas comerciais que resultam em abusos e evidências de que há um "*escopo para o desenvolvimento e o aprimoramento das atuais proteções e medidas de mitigação*", além do potencial para desenvolver políticas no futuro[4].

[3] Consulte as Recomendações de Devida Diligência das Agências Legais Fiscalizadoras (outubro de 2019) e as 12 Recomendações das Agências Legais Fiscalizadoras (1º de março de 2012)

[4] Consulte o comentário do GAC (19 de setembro de 2017) sobre o Relatório Final da Análise Estatística sobre Abusos do DNS em gTLDs.

Além disso, preocupações com a capacidade de mitigar de maneira eficiente os Abusos do DNS foi destacada nos círculos de agências legais fiscalizadoras, segurança cibernética, proteção do consumidor e proteção intelectual[5] em decorrência da entrada em vigor do GDPR (General Data Protection Regulation, Regulamento Geral de Proteção de Dados) da União Europeia e os esforços para a alterar o sistema de WHOIS, uma ferramenta essencial na investigação de crimes e abusos, de modo a estar em conformidade com o GDPR. Mais recentemente, a emergência de saúde mundial da COVID-19 comprovou uma ilustração de que os desafios existentes relacionados aos registros de domínios aumentaram, inclusive uma pequena porcentagem [6] em apoio a diversas finalidades fraudulentas oportunistas.

Os Comitês Consultivos da ICANN, particularmente o GAC, o SSAC e o ALAC, e diversos terceiros afetados pediram que a Organização ICANN e a Comunidade da ICANN tomasse providências[7].

Essas providências exigiriam que a comunidade da ICANN encontrasse algum tipo de consenso sobre várias questões em aberto. As discussões sobre a mitigação de abuso e um possível trabalho de política na Comunidade da ICANN geralmente giram em torno dos seguintes tópicos:

- **Definição de Abuso do DNS:**
  O que constitui abuso considerando o âmbito da ICANN e dos contratos dela com Registros e Registradores?
- **Detecção e emissão de relatórios de abuso do DNS (perspectiva de transparência e conscientização):**
  Como podemos garantir que o Abuso do DNS seja detectado e informado às partes interessadas relevantes, inclusive consumidores e usuários da Internet?
- **Prevenção e mitigação de Abuso do DNS (perspectiva da eficiência):**
  Quais ferramentas e procedimentos a Organização ICANN, os participantes do setor e as partes interessadas podem usar para reduzir a ocorrência de abusos e responder adequadamente quando eles ocorrerem? Quem é responsável por quais partes do quebra-cabeça, e como diferentes partes podem cooperar entre si?

O GAC, em um esforço para melhorar a segurança e a estabilidade para os usuários da Internet em geral, talvez queira participar mais ativamente na discussão sobre esses tópicos (documentado em detalhes neste resumo) para que possamos avançar em direção a soluções mais eficientes para a prevenção e a mitigação de abusos.

---

[5] Consulte a Seção III.2 e IV.2 no Comunicado do GAC de Barcelona (25 de outubro de 2018) que indica algumas pesquisas sobre o impacto nas agências legais fiscalizadoras na seção 5.3.1 do Relatório Preliminar da Equipe de Revisão de RDS (31 de agosto de 2018) e em uma publicação dos Grupos de Trabalho sobre Anti-phishing e Antiabuso de Mensagens, Malware e Dispositivos Móveis (18 de outubro de 2018)

[6] Conforme relatado pelos líderes do Grupo de Partes Interessadas de Registradores ao GAC em 9 de abril de 2020

[7] Consulte a discussão sobre Abusos do DNS e Proteções do Consumidorhttps://www.icann.org/resources/pages/gdd-summit-session-recordings-2019-05-08-en durante a Cúpula da GDD (7 a 8 de maio de 2019).

Proposta da liderança para ações do GAC durante o ICANN68

1. **Revisar as lições aprendidas** até o momento **com Abusos do DNS relacionados à COVID-19**, conforme relatado pelas partes afetadas, inclusive autoridades públicas, registradores, operadores de ccTLDs e a Organização ICANN, **e se preparar para interagir com a Comunidade da ICANN, conforme apropriado,** começando pela Sessão de Plenária Entre Comunidades sobre Abusos do DNS e Registros Maliciosos durante a COVID-19, planejada para 22 de junho de 2020, como parte do ICANN68.

2. **Deliberar sobre possíveis etapas futuras para solucionar os problemas gerais de política pública relacionados a Abusos do DNS**, conforme identificado em contribuições anteriores do GAC, e, **em particular, considerar entrar em contato** com o Conselho da GNSO, o ALAC, a ccNSO e possivelmente a Diretoria da ICANN **sobre possíveis formas de lidar com as recomendações da Revisão de CCT relacionadas a Abusos do DNS antes do lançamento das rodadas subsequentes de novos gTLDs**, de maneira consistente com os Conselhos no Comunicado do GAC de Montreal (6 de novembro de 2019).

3. **Debater o status** de consideração e implementação **de recomendações relacionadas a Abusos do DNS emitidas pelas equipes de Revisão de CCT e do RDS-WHOIS2**, tendo em vista a Ação da Diretoria da ICANN, conforme relatado em:
    a. Scorecard de Ação da Diretoria às recomendações da Revisão de CCT (1º de março de 2019)
    b. Scorecard de Ação da Diretoria às recomendações da Revisão de RDS-WHOIS2 (25 de fevereiro de 2020)

4. **Considerar o progresso das principais Iniciativas de Mitigação de Abusos do DNS, em termos mais gerais, na Comunidade da ICANN** e em especial pelas Partes Contratadas, Operadores de ccTLDs e a Organização ICANN, inclusive com o objetivo de promover padrões elevados em práticas e contratos:
    a. **Implementação de medidas voluntárias por Registros e Registradores**, de acordo com a Estrutura para Lidar com Abusos liderada pelo setor
    b. **Implementação de medidas proativas antiabuso pelos Operadores de ccTLDs** que possam informar as práticas de registros de gTLDs
    c. **Auditoria de Conformidade Contratual de Registradores** com relação a Ameaças de Segurança do DNS que deveria seguir a conclusão de uma auditoria semelhante de Registros
    d. Aprimoramentos do DAAR (Domain Abuse Activity Reporting, Geração de Relatórios de Atividade de Abuso de Domínios) da ICANN, conforme discutido anteriormente por Registros, o GAC e o SSAC

Acontecimentos relevantes

Visão geral dos acontecimentos recentes

- **A crise da COVID-19 levou a interações entre o GAC e as partes interessadas afetadas**, que apresentaram as diversas **iniciativas para responder e coordenar as respostas** contra atividade criminosas e fraudulentas:
    - **A liderança do GAC** relatou em uma discussão (9 de abril) solicitadas por líderes do RrSG (Registrar Stakeholder Group, Grupo de Partes Interessadas de Registradores), e debateu a questão em mais detalhes em uma teleconferência conjunta da liderança (3 de junho de 2020), em preparação para o ICANN68.
    - Como parte de uma resposta a possíveis atividades fraudulentas relacionadas à COVID-19, os **Registradores** relataram desafios para avaliar as fraudes em jurisdições relevantes e buscaram assistência das autoridades públicas. O RrSG documentou as abordagens compartilhadas de Registradores à crise da COVID-19 para ajudar seus membros.
    - **Os membros do GAC foram convidados a compartilhar recursos relevantes** aplicados por suas respectivas autoridades públicas, como os que foram compartilhados pelas agências legais fiscalizadoras (FBI dos EUA, NCA do Reino Unido e Europol) e agências de proteção do consumidor (FTC dos EUA)
    - A **Comissão Europeia** relatou iniciativas contínuas em colaboração com os estados-membros da União Europeia, Europol, ccTLDs e registradores para facilitar os relatórios, a revisão desses e sua referência às jurisdições relevantes durante a adoção de um formulário padronizado para relatar domínios/conteúdo relacionados à COVID-19 e o estabelecimento de um ponto de contato único para as autoridades relevantes do estados-membros.
    - **Operadores de ccTLDs** do mundo todo deverão informar o GAC (4 a 5 de junho de 2020) sobre as lições aprendidas em suas operações durante a crise
    - Um resumo do GAC pelo **Escritório do CTO da ICANN** (OCTO), planejado para antes do ICANN68, deverá ilustrar as iniciativas e os recursos da ICANN dedicados a apoiar a resposta das partes contratadas

- Enquanto isso, as **Partes Contratadas, o SSAC (Security and Stability Advisory Committee, Comitê Consultivo de Segurança e Estabilidade) da ICANN e a Organização ICANN iniciaram um novo trabalho** relacionado à resolução de Ameaças à Segurança:
    - Conforme relatado pelo Grupo de Trabalho de Segurança Pública do GAC durante o encontro ICANN67, o **Grupo de Partes Interessadas de Registradores** publicou um Guia para o Relatório de Abusos de Registradores
    - A Estrutura para Lidar com Abusos do DNS (17 de outubro de 2019) proposta como uma **iniciativa voluntária por partes interessadas importantes do setor de DNS** tem agora 56 signatários (dados de 29 de março de 2020).

- O **SSAC** iniciou uma Equipes de Trabalho sobre Abusos do DNS em que um representante do PSWG foi convidado a participar.
- A **Organização ICANN**, como parte da implementação do Planejamento Estratégico do AF21-25, anunciou o lançamento de um Grupo de Estudo Técnico de Iniciativas para a Facilitação de Segurança do DNS (6 de maio de 2020) para *"explorar ideias sobre o que a ICANN pode e deve fazer para aumentar o nível de colaboração e integração com partes interessadas do ecossistema do DNS para melhorar o perfil de segurança do DNS"*. A recomendações são esperadas até maio de 2021.

- Desde o encontro ICANN66, vários **processos da comunidade da ICANN consideraram novas recomendações relacionadas a Abusos do DNS**, e algumas delas receberam pareceres do GAC e outras poderão estar sujeitas a acompanhamento do GAC:
  - Depois que as Recomendações Finais da **Equipe de Revisão do RDS-WHOIS2** (3 de setembro de 2019), cuja relevância para a mitigação de Abusos do DNS foi destacada em um comentário do GAC (23 de dezembro de 2019), foram consideradas pela Diretoria da ICANN de acordo com o Scorecard de Ação da Diretoria (25 de fevereiro de 2020) e como parte de suas resoluções 2020.02.25.01 – 2020.02.25.06: 15 recomendações foram aceitas, 4 receberam o status pendente, 2 foram repassadas à GNSO e 2 foram rejeitadas.
  - **A Equipe de Revisão de SSR2** apresentou um Relatório Preliminar (24 de janeiro de 2020) com um foco significativo em medidas para prevenir e mitigar Abusos do DNS. O comentário do GAC (3 de abril de 2020) endossou muitas das recomendações, particularmente as relacionadas a aprimoramentos do DAAR (Domain Abuse Activity Reporting, Geração de Relatórios de Atividade de Abuso de Domínios) e ao fortalecimento de mecanismos de conformidade. No momento, as recomendações finais do Equipe de Revisão de SSR2 são esperadas até outubro de 2020 (de acordo com deliberações recentes)
  - **O Grupo de Trabalho do Processo de Desenvolvimento de Políticas para Procedimentos Subsequentes de Novos gTLDs da GNSO** recentemente comunicou (29 de abril de 2020) que "*não planeja fazer nenhuma recomendação com relação à mitigação de abusos de nomes de domínio, além de afirmar que qualquer iniciativa futura dessa natureza precisa se aplicar a gTLDs novos e existentes (e possivelmente a ccTLDs)".* Essa afirmação é independente das recomendações relevantes endereçadas ao grupo pela Equipe de Revisão de CCT, também apoiada pela Ação da Diretoria da ICANN sobre essas recomendações, bem como o Conselho do Comunicado do GAC de Montreal (6 de novembro de 2019) e outros pareceres do GAC, conforme registrado no Comunicado do GAC do ICANN67 (16 de março de 2020). Uma reunião recente do Conselho da GNSO (21 de março de 2020) discutiu a possibilidade de iniciar um CCWG (Cross-Community Working Group, Grupo de Trabalho Entre Comunidades) e talvez um PDP subsequente da GNSO, caso sejam necessários novos requisitos contratuais. O Conselho não abordou uma proposta informal feita pela liderança do GAC (12 de maio de 2020) para considerar uma

discussão de afinidades entre especialistas relevantes, inclusive operadores de ccTLDs, a fim de estabelecer um escopo para qualquer iniciativa futura de política.

Assuntos — definição de Abusos do DNS

Conforme destacado mais recentemente durante a Cúpula da GDD (7 a 9 de maio de 2019), **não há um acordo de toda a Comunidade sobre o que constitui "Abuso do DNS"**, em parte devido às preocupações de algumas partes interessadas com os impactos nos direitos dos usuários e nas funções básicas das partes contratadas, bem como de que a ICANN ultrapasse seu escopo.[8]

No entanto, de acordo com a Equipe de Revisão de CCT, existe um **consenso sobre o que constitui "Abuso de segurança do DNS" ou "Abuso de segurança do DNS na infraestrutura do DNS"**, pois entende-se que isso inclui *"formas mais técnicas de atividades maliciosas"*, como malware, phishing e botnets, além de spam *"quando usado como um método de entrega de outras formas de abuso"* [9].

Recentemente, **o departamento de Conformidade Contratual da ICANN referiu-se a "Abuso da infraestrutura do DNS" e "Ameaças à segurança"** em suas comunicações sobre auditorias de Registros e Registradores com relação à implementação de disposições contratuais previstas no Contrato de Registro de Novos gTLDs (Especificação 11 3b), que se refere a "*ameaças à segurança, como pharming, phishing, malware e botnets*"[10] — e no Contrato de Credenciamento de Registradores (Seção 3.18), que se refere a "*contatos de abuso*" e "*relatórios de abuso*" especificamente, mas incluindo a expressão "atividade ilegal" no escopo.

Do ponto de vista do GAC, a definição de "ameaças à segurança" incluída no Contrato de Registro de Novos gTLDs é de fato a transcrição exata da **definição apresentada no Conselho de Proteções do GAC sobre "verificações de segurança"**, aplicável a todos os novos gTLDs no Comunicado de Pequim (11 de abril de 2013).

Após a resolução da Diretoria (1º de março de 2019) orientando a Organização ICANN a "*facilita[r] o trabalho da comunidade para elaborar uma definição de 'abuso' a fim de ajudar nas próximas ações para essa recomendação*"[11] e a desenvolver atividades com a equipe de Proteções do Consumidor da Organização ICANN, **espera-se que mais discussões sejam realizadas sobre a definição de abuso antes e durante o encontro ICANN66**, em Montreal.

Particularmente, durante um webinário que antecedeu o ICANN66 em 15 de outubro de 2019, **o PSWG e as Partes Contratadas discutiram os assuntos atuais e as práticas do setor**. Em preparação para esse webinário, o Grupo de Partes Interessadas de Registros enviou uma Carta Aberta (19 de agosto de 2019) apresentando as opiniões de registros sobre a definição de Abusos

---

[8] De fato, a definição de Mitigação de Abuso pode ter várias consequências no que diz respeito ao escopo das atividades supervisionadas pelos contratos e pelas políticas da ICANN. Embora os governos e outras partes interessadas tenham receio quanto ao impacto de abusos do DNS no interesse público, inclusive na segurança do público e na violação de direitos de propriedade intelectual, os registros e os registradores estão preocupados com as restrições nas atividades comerciais deles, na capacidade de competir, no aumento dos custos operacionais e na responsabilidade por consequências que poderão afetar os registrantes quando ações forem tomadas nos domínios abusivos. As partes interessadas não comerciais, por outro lado, estão preocupadas com a violação da liberdade de expressão e os direitos de privacidade de registrantes e usuários da Internet, e compartilham com as partes contratadas receios de que a ICANN ultrapasse a missão dela.

[9] Consulte a pág. 88 do Relatório Final da Revisão de CCT (8 de setembro de 2018), conforme destacado mais recentemente na Declaração do GAC sobre Abusos do DNS (18 de setembro de 2019)

[10] O Conselho, Contrato de Registro de Novos gTLDs, Especificação 11 (3)(b) (8 de junho de 2017) apresenta uma definição para "ameaças à segurança", que inclui "*pharming, phishing, malware, botnets e outros tipos de ameaças à segurança*".

[11] Consulte a pág. 5 do Scorecard da Ação da Diretoria com relação às Recomendações Finais da equipe de CCT

do DNS, as opções limitadas disponíveis para os registros usarem contra ameaças à segurança e suas preocupações com os Relatórios de Atividade de Abuso de Domínios da ICANN. Em resposta, o GAC enviou uma Declaração sobre Abusos do DNS (18 de setembro), bem como o Grupo Constituinte Corporativo (28 de outubro).

Assuntos — conhecimento e transparência: participações da comunidade com relação a abusos do DNS

O GAC e o PSWG (Public Safety Working Group, Grupo de Trabalho sobre Segurança Pública) têm realizado várias conversas entre comunidades nos encontros da ICANN nos últimos anos com o objetivo de **aumentar o conhecimento e explorar soluções com os especialistas relevantes**. Mais recentemente, os líderes de SOs/ACs (Supporting Organizations and Advisory Committee, Organizações de Apoio e Comitês Consultivos) da ICANN e o ALAC realizaram reuniões com uma excelente participação sobre o assunto.

- Durante o ICANN57, em Hyderabad, (5 de novembro de 2016), o PSWG do GAC realizou uma sessão de tópico de maior interesse sobre a Mitigação de Abusos em gTLDs, que foi estruturada como uma troca de opiniões entre os membros da Comunidade da ICANN e destacou:
    - a ausência de um entendimento comum sobre o que é Abuso do DNS;
    - a diversidade de modelos de negócios, práticas e habilidades que influenciam as abordagens para mitigar abusos; e
    - a necessidade de haver mais cooperação entre os participantes do setor, que seria apoiada por dados compartilhados sobre ameaças à segurança.

- Durante o ICANN58, em Copenhague (13 de março de 2017), o PSWG do GAC moderou uma Sessões entre Comunidades Para a Mitigação Eficiente de Abusos do DNS: prevenção, mitigação e resposta, que tratou das recentes tendências em Abusos do DNS, particularmente phishing, bem como em comportamentos, como "salto de domínio" entre registradores e TLDs, que podem exigir respostas mais coordenadas e sofisticadas no setor. A sessão também serviu para destacar:
    - a emergente iniciativa DAAR (Domain Abuse Activity Reporting, Geração de Relatórios de Atividade de Abuso de Domínios),
    - a colaboração contínua entre as equipes de SSRT (Security and Stability Review Team, Equipe de Revisão de Segurança e Estabilidade) e Conformidade Contratual da ICANN, e
    - a oportunidade de utilizar os rendimentos de leilões de novos gTLDs para financiar as necessidades da mitigação de abusos

- Durante o ICANN60, em Abu Dhabi, (30 de outubro de 2017), o PSWG organizou uma Sessão entre Comunidades sobre Emissão de Relatórios de Abusos do DNS para Formulação de Políticas com Base em Fatos e Atenuação Eficiente para discutir o estabelecimento de mecanismos de emissão de relatórios sobre Abusos do DNS que fossem confiáveis, públicos e permitissem ações viáveis, a fim de evitar e mitigar abusos, além de facilitar a elaboração de políticas baseadas em evidências. A sessão confirmou a necessidade de publicar dados confiáveis e detalhados sobre Abusos do DNS, como os contidos na ferramenta de DAAR (Domain Abuse Activity Reporting, Geração de Relatórios

de Atividade de Abuso de Domínios). O PSWG considerou também elaborar possíveis princípios para o GAC[12].

- Durante o ICANN66 em Montreal (6 de novembro de 2019), a Comunidade da ICANN realizou um Sessão de Plenária Entre Comunidades sobre Abusos do DNS

- Durante o Encontro Virtual do ICANN67 (9 de março de 2020), o ALAC realizou duas sessões remotas com vários participantes da Comunidade da ICANN, uma apresentando uma introdução a Abusos do DNS (incluindo um vídeo educacional) e um revisando em prática a execução de Conformidade Contratual em resposta a casos típicos de Abusos do DNS

Assuntos — conhecimento e transparência: estudos sobre Abuso do DNS

Várias proteções relacionadas a Abusos do DNS foram colocadas no Programa de Novos gTLDs por meio de novos requisitos[13] adotados pela Organização ICANN de acordo com o memorando sobre Mitigação de Condutas Maliciosas (3 de outubro de 2009) e o Conselho de Proteção do GAC sobre as verificações de segurança.

Com base na avaliação da Organização ICANN sobre a eficiência das Proteções do Programa de Novos gTLDs (18 de julho de 2016), que contou com a contribuição do GAC (20 de maio de 2016), a Equipe de Revisão de CCT buscou uma análise comparativa mais abrangente dos índices de abuso em gTLDs novos e legados, incluindo uma análise estatística inferida de hipóteses, como as correlações entre os índices de abuso e os preços para a venda de nomes de domínio.

As conclusões dessa Análise Estatística sobre Abusos do DNS em gTLDs (9 de agosto de 2017) foram enviadas para comentários públicos. As contribuições da Comunidade foram relatadas (13 de outubro de 2017) como construtivas, elogiando o rigor científico da análise e solicitando que mais estudos como esse fossem realizados.

Nos seus comentários (19 de setembro de 2017), o GAC destacou, entre outras conclusões, que:

- O estudo deixou claro que há problemas sérios de abuso no DNS:
    - Em certos novos gTLDs, mais de 50% dos registrantes são abusivos
    - Cinco novos gTLDs foram responsáveis por 58,7% de todos os domínios de phishing em novos gTLDs colocados em uma lista negra
- Os abusos estão correlacionados às políticas dos Operadores de Registro:
    - Os operadores de registro dos novos gTLDs com o maior número de abusos são concorrentes diretos de preços;
    - As partes maliciosas preferem registrar domínios em novos gTLDs comuns (abertos para registro público), e não em novos gTLDs de comunidades (com restrições para quem pode registrar os nomes de domínio)

---

12 Consulte o Anexo 1: Princípios de Mitigação de Abusos no Resumo do GAC do ICANN60 sobre Abusos do DNS e relatório da sessão no Comunicado do GAC de Abu Dhabi (pág. 3)

13 Investigar os operadores de registro, exigir um plano demonstrado para a implementação de DNSSEC, proibir o uso de caracteres curinga, remover registros glue órfãos quando uma entrada no servidor de nomes for removida da zona, exigir a manutenção dos registros de WHOIS thick, a centralização do acesso de arquivos de zona, exigir procedimentos e contatos de abuso no nível do registro documentados.

- Existe o potencial para o futuro desenvolvimento de políticas para:
    - Rodadas subsequentes de novos gTLDs, relacionadas a evidências de que o risco varia nas categorias de TLDs, além do rigor da política de registro
    - O aprimoramento das atuais medidas de mitigação e proteções contra abusos, conforme indicado pela análise estatística
- A ICANN deve continuar usando, e expandir esse uso, de análises estatísticas e dados para medir e compartilhar informações com a comunidade sobre os níveis de abuso do DNS.

Em 17 de outubro de 2019, um estudo de Abuso Criminoso de Registros em Massa de Nomes de Domínio e Acesso a Informações de Contato foi publicado por uma empresa de consultorias (Interisle Consulting Group) com relevância direta para as discussões em andamento da comunidade e explorou:

- Como os criminosos cibernéticos utilizam os serviços de registro em massa para "explorar" um número enorme de nomes de domínio em seus ataques.
- Efeitos da política interina da ICANN que editou as informações do ponto de contato do WHOIS para manter a conformidade com o GDPR com relação às investigações de crimes cibernéticos
- Recomendações de políticas para consideração pela Organização ICANN e a comunidade

Assuntos — conhecimento e transparência: DAAR (Domain Abuse Activity Reporting, Geração de Relatórios de Atividade de Abuso de Domínios)

O projeto de Geração de Relatórios de Atividade de Abuso de Domínios da Organização ICANN começou como um projeto de pesquisa simultâneo à conversa do GAC e do PSWG com a Comunidade e a Diretoria da ICANN sobre a eficiência da mitigação de abusos do DNS, entre o ICANN57 (novembro de 2016) e o ICANN60 (novembro de 2017).[14]

A finalidade declarada do DAAR é "*relatar as atividades de ameaças à segurança para a comunidade da ICANN, que poderá usar os dados para tomar decisões sobre políticas com informações relevantes*". Isso é feito desde janeiro de 2018 com a publicação de relatórios mensais, com base na compilação de dados de registro de TLDs incluindo informações de um conjunto enorme de feeds de dados de ameaças à segurança e reputação de alta confiança.[15]

Dessa forma, o DAAR está contribuindo para o requisito identificado pelo GAC da publicação de *"dados detalhados e confiáveis sobre Abuso do DNS"* mencionado no Comunicado do GAC de Abu Dhabi (1º de novembro de 2017). No entanto, conforme destacado em uma carta recente do M3AAWG[16] para a Organização ICANN (5 de abril de 2019), ao não incluir as informações de ameaças à segurança de cada registrador para cada TLD, o DAAR ainda não atende às expectativas

[14] Consulte as sessões entre comunidades lideradas pelo PSWG do GAC durante o ICANN57 (novembro de 2016), o ICANN58 (março de 2017) e o ICANN60 (outubro de 2017), bem como as perguntas enviadas à Diretoria da ICANN sobre a eficiência das proteções de abusos do DNS no Comunicado de Hyderabad (8 de novembro de 2016), as perguntas de acompanhamento no Comunicado do GAC de Copenhague (15 de março de 2017) e um conjunto de respostas preliminares (30 de maio de 2017) da Organização ICANN.

[15] Para saber mais, consulte https://www.icann.org/octo-ssr/daar-faqs

[16] Grupo de Trabalho de Mensagens, Malware e Antiabuso em Dispositivos Móveis

dos membros do PSWG do GAC e dos parceiros de segurança cibernética de fornecer informações para ações viáveis.

Recentemente, os registros relataram em uma Carta Aberta (19 de agosto de 2019) uma interação com Escritório do CTO da ICANN "*para analisar o DAAR com o objetivo de recomendar aprimoramentos ao Escritório do CTO a fim de garantir que o DAAR atenda melhor sua finalidade intencionada e fornecer à comunidade da ICANN um recurso valioso*". Embora os registros reconheçam que "*alguns membros da comunidade possam depender dos dados fornecidos pela Geração de Relatórios de Atividade de Abuso de Domínios da ICANN (DAAR) para corroborar alegações de Abusos do DNS sistêmicos ou amplos*", eles acreditam que "*a ferramenta tem limitações significativas, não é capaz de assegurar evidências de relatórios precisas e confiáveis de ameaças à segurança e ainda não atende aos seus objetivos*".

Assuntos — eficiência: atuais proteções contra abusos do DNS em contratos de Registros e Registradores

Com base nas Recomendações de Devida Diligência das Agências Legais Fiscalizadoras (outubro de 2009), o GAC buscou a **inclusão das Proteções para a Mitigação de Abusos do DNS nos contratos da ICANN** com Registros e Registradores:

- O Contrato de Credenciamento de Registradores de 2013 (17 de setembro de 2013) foi aprovado pela Diretoria da ICANN (27 de junho de 2013) após a inclusão das disposições que abordavam as 12 Recomendações das Agências Legais Fiscalizadoras (1º de março de 2012)
- O Contrato de Registro de Novos gTLDs foi aprovado pela Diretoria da ICANN (2 de julho de 2013) após a inclusão de disposições alinhadas ao Conselho de Proteções do GAC incluído no Comunicado de Pequim (11 de abril de 2013), de maneira consistente com a Proposta da Diretoria da ICANN de Implementação de Proteções do GAC Aplicáveis a Todos os Novos gTLDs (19 de junho de 2013)

Após os primeiros anos de operação dos novos gTLDs, durante o ICANN57 **o GAC identificou uma série de disposições e proteções relacionadas para a qual não conseguiu avaliar a eficiência**. Em decorrência disso, no Comunicado de Hyderabad (8 de novembro de 2016) o GAC solicitou esclarecimentos à Diretoria da ICANN sobre a implementação. Isso resultou em um diálogo entre o GAC e a Organização ICANN, perguntas de acompanhamento no Comunicado do GAC de Copenhague (15 de março de 2017) e um conjunto de respostas preliminares (30 de maio de 2017) que foram discutidos em uma teleconferência entre o GAC e o CEO da ICANN (15 de junho de 2017). Várias perguntas continuaram em aberto e novas perguntas foram identificadas, conforme consta em um documento de trabalho posterior (17 de julho de 2017).

Entre os tópicos pendentes de interesse ao GAC, um Conselho, Contrato de Registro de Novos gTLDs, Especificação 11 (3)(b) foi publicado em 8 de junho de 2017 em resposta a perguntas de alguns operadores de registro que buscavam orientação sobre como garantir a conformidade com a Seção 3b da Especificação 11 do Contrato de Registro de Novos

gTLDshttps://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html - specification11. **O Conselho apresenta uma abordagem voluntária que pode ser adotada pelos operadores de registro** para realizar análises técnicas a fim de avaliar as ameaças à segurança e gerar relatórios estatísticos, conforme exigido pela Especificação 11 3(b).

Como parte das **auditorias regulares realizadas pelo departamento Contratual da ICANN**, uma auditoria direcionada de 20 gTLDs sobre o "*processo, procedimentos e gerenciamento da infraestrutura do DNS"* deles, entre março e setembro de 2018, revelou que "*havia relatórios de segurança e análises incompletos para 13 TLDs (Top Level Domains, Domínios de Primeiro Nível), bem como a ausência de procedimentos padronizados ou documentos para o gerenciamento de abusos e nenhuma ação tomada quanto às ameaças identificadas*"[17]. Pouco tempo depois, em novembro de 2018, uma Auditoria sobre Abusos na Infraestrutura do DNS de quase todos os gTLDs foi iniciada para "*garantir que as partes contratadas cumpram suas obrigações contratuais com relação a ameaças à segurança e abusos na infraestrutura do DNS"*. Em seu relatório da auditoria mais recente (17 de setembro de 2019), a ICANN concluiu que:

- a grande maioria dos operadores de registro está comprometida em resolver as ameaças à segurança do DNS.
- A maior parte das ameaças à segurança do DNS está concentrada em um número relativamente pequeno de operadores de registro.
- Alguns Operadores de Registro interpretam o texto contratual da Especificação 11 3(b) de maneira a dificultar o julgamento sobre se as iniciativas deles para mitigar as ameaças à segurança do DNS estão em conformidade e são eficazes.

As **partes contratadas têm acompanhado os problemas com essas auditorias** como excedendo o escopo das suas obrigações contratuais[18]. A Organização ICANN indicou que iniciará uma auditoria dos registradores com foco nas ameaças à segurança do DNS.

[17] Conforme relatado na postagem de blog de 8 de novembro de 2018, Conformidade Contratual: como lidar com abusos na infraestrutura do DNS: https://www.icann.org/news/blog/contractual-compliance-addressing-domain-name-system-dns-infrastructure-abuse

[18] Consulte a correspondência do RySG (Registries Stakeholder Group, Grupo de Partes Interessadas de Registros) (2 de novembro de 2019) com a seguinte resposta da Organização ICANN (8 de novembro), e nos comentários publicados na página de comunicado (15 de novembro): os registros identificaram problemas com as perguntas da auditoria considerando uma ação de execução ameaçadora que excede o escopo das obrigações contratuais deles [particularmente na Especificação 11 3b] e indicaram relutância para "*compartilhar com a Organização ICANN e a comunidade informações relevantes sobre nossos esforços aplicados para combates abusos do DNS […] como parte de um esforço de Conformidade da ICANN que vai além do que é permitido no Contrato de Registro*"

Eficiência: estrutura não vinculativa para Registros responderem a ameaças à segurança

Como parte do Programa de Novos gTLDs, a Diretoria da ICANN decidiu (25 de junho de 2013) incluir as chamadas "verificações de segurança" (Conselho de Proteções do GAC do Comunicado de Pequim) na Especificação 11 do Contrato de Registro de Novos gTLDs. No entanto, como foi determinado que essas disposições não têm os detalhes da implementação, a ICANN decidiu solicitar a participação da comunidade para elaborar uma estrutura para "*Operadores de Registro responderem a riscos de segurança identificados que representem risco real de dano (…)*".
Em julho de 2015, a ICANN montou uma Equipe Redatora composta de voluntários de Registros, Registradores e do GAC (inclusive com membros do PSWG) que elaborou a Estrutura para Operadores de Registros Responderem a Ameaças à Segurança publicada em 20 de outubro de 2017, depois de passar por um período de comentários públicos.

Esta estrutura é um instrumento voluntário não vinculativo projetado para articular orientações que possam ser usadas pelos registros para responder a ameaças à segurança identificadas, inclusive relatórios de agências legais fiscalizadoras. Ela introduz uma janela de no máximo 24 horas para responder a solicitações de alta prioridade (ameaça iminente à vida humana, infraestrutura essencial ou exploração infantil) de uma *"origem legítima e confiável"*, como uma *"autoridade de agência legal fiscalizadora governamental ou agência de segurança pública de uma jurisdição apropriada"*.

De acordo com sua recomendação 19, a Equipe de Revisão de CCT deferiu a tarefa de realizar uma avaliação da eficiência da Estrutura para uma revisão subsequente[19], uma vez que a Estrutura não existia por um período longo suficiente para avaliar sua eficiência.

Eficiência: medidas proativas e prevenção contra abusos sistêmicos

Com base em sua análise do cenário de Abusos do DNS,[20] incluindo a consideração do Relatório da ICANN sobre as Proteções do Programa de Novos gTLDs (15 de março de 2016) e a Análise Estatística Independente sobre Abusos do DNS (9 de agosto de 2017), a Equipe de Revisão de CCT recomendou, com relação a Abusos do DNS:

- A inclusão de **disposições nos Contratos de Registros para incentivar a adoção de medidas antiabuso proativas** (Recomendação 14)
- A inclusão de disposições contratuais com o objetivo de **prevenir contra o uso sistêmico de registradores ou registros específicos** para Abuso de Segurança do DNS, inclusive com limites de abusos que, se ultrapassados, acionarão consultas de conformidade automáticas, e considerar uma possível DADRP (DNS Abuse Dispute Resolution Policy, Política de Resolução de Disputas de Abusos do DNS), se a comunidade determinar que a Organização ICANN não é indicada ou não é capaz de exigir essas disposições (Recomendação 15)

---

19 Recomendação 19 da Revisão de CCT: *A próxima CCT deverá revisar a "Estrutura para Operadores de Registro responderem a ameaças à segurança" e avaliar se a estrutura é um mecanismo suficientemente claro e eficiente para mitigar abusos, oferecendo medidas específicas e sistêmicas em resposta a ameaças de segurança*

20 Consulte a Seção 9 sobre Proteções (pág. 88) do Relatório Final da Revisão de CCT (8 de setembro de 2018)

A Diretoria da ICANN decidiu (1º de março de 2019) colocar essas recomendações com o status "Pendentes", já que orientavam a Organização ICANN a "*facilita[r] o trabalho da comunidade para elaborar uma definição de 'abuso' a fim de ajudar nas próximas ações para essa recomendação*"[21].

Posições atuais

As posições atuais do GAC são listadas abaixo, em ordem cronológica inversa:

- Comentário do GAC (3 de abril de 2020) sobre a Versão Preliminar do Relatório da Equipe de Revisão do SSR2
- Comentário do GAC (23 de dezembro de 2019) sobre as Recomendações Finais da Revisão do RDS-WHOIS2
- Declaração do GAC sobre o DNS (18 de setembro de 2019)
- Comentário do GAC (11 de dezembro de 2019) sobre as Recomendações Finais da Revisão do CCT
- Comentário do GAC (16 de janeiro de 2018) sobre as Novas Seções do Relatório Preliminar da Equipe de Revisão de CCT (27 de novembro de 2017)
- Comentário do GAC sobre a Análise Estatística de Abusos do DNS em gTLDs (19 de setembro de 2017)
- Comentário do GAC sobre o Relatório Inicial do SADAG (21 de maio de 2016)
- Comunicado do GAC de Barcelona (25 de outubro de 2018) em particular as seções III.2 do Grupo de Trabalho de Segurança Pública do GAC (pág. 3) e IV.2 Legislação sobre Proteção de Dados e WHOIS (pág. 5)
- Comunicado do GAC de Copenhague (15 de março de 2017) inclusive o Conselho sobre Mitigação de Abusos solicitando respostas para o Scorecard de Acompanhamento do GAC relacionado ao Anexo 1 do Comunicado do GAC de Hyderabad (pág. 11 a 32)
- Comunicado do GAC de Hyderabad (8 de novembro de 2016) inclusive o Conselho sobre Mitigação de Abusos solicitando respostas para o Anexo 1 — Perguntas à Diretoria da ICANN sobre a mitigação de abuso do DNS por parte da ICANN e partes contratadas (pág. 14 a 17)
- Comunicado do GAC de Pequim (11 de abril de 2013), em particular as proteções de "verificações de segurança" aplicáveis a todos os novos gTLDs (pág. 7)
- Comunicado do GAC de Dakar (27 de outubro de 2011) seção III. Recomendações de LEAs (Law Enforcement Agencies, Agências Legais Fiscalizadoras)
- Comunicado do GAC de Nairóbi (10 de março de 2010) seção VI. Recomendações de devida diligência das agências legais fiscalizadoras
- Recomendações de LEAs sobre Aditamentos aos Contratos de Registros (1º de março de 2012)

[21] Consulte a pág. 5 do Scorecard da Ação da Diretoria com relação às Recomendações Finais da equipe de CCT

- Recomendações de Devida Diligência das Agências Legais Fiscalizadoras (outubro de 2009)

Documentos de referência importantes

- Scorecard de Ação da Diretoria da ICANN sobre as Recomendações Finais da Revisão do RDS-WHOIS2 (25 de fevereiro de 2020)
- Scorecard de Ação da Diretoria da ICANN sobre as Recomendações Finais da Revisão de CCT (1º de março de 2019)
- Recomendações e Relatório Final da Revisão de CCT (8 de setembro de 2018), em particular a Seção 9 sobre Proteções (pág. 88)
- Análise Estatística de Abusos do DNS em gTLDs (9 de agosto de 2017)
- Perguntas do GAC sobre a Mitigação de Abusos e Respostas Preliminares da ICANN (30 de maio de 2017) conforme o Conselho no Comunicado do GAC de Hyderabad (8 de novembro de 2016) e Acompanhamento no Comunicado do GAC de Copenhague (15 de março de 2017)

Administração do documento

Encontro	Fórum Virtual de Políticas do ICANN68, de 22 a 25 de junho de 2020
Título	Mitigação de abusos do DNS
Distribuição	Membros do GAC (antes do encontro) e público (após o encontro)
Data de distribuição	Versão 1: 3 de junho de 2020