ICANN | GAC
Governmental Advisory Committee

ICANN 70 VIRTUAL COMMUNITY FORUM

Mitigação de abusos do DNS

Sessões 8 e 16

Índice

Objetivos da sessão

O GAC analisará acontecimentos recentes na comunidade da ICANN, incluindo a conclusão da revisão de SSR2 e a do PDP de procedimentos subsequentes para definir as próximas etapas para garantir as medidas adequadas a serem tomadas para prevenir e reduzir o abuso do DNS em gTLDs, incluindo a consideração de propostas concretas para a melhoria das cláusulas contratuais e sua aplicação.

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 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. No entanto, é importante observar que até mesmo a definição exata de "Abuso do DNS" é um assunto para debate.

Embora as partes interessadas e a comunidade da ICANN no geral parecem concordar que o abuso do DNS é um problema que precisa ser resolvido, existem opiniões diferentes sobre as responsabilidades das partes relevantes. Por exemplo, os registros e registradores estão preocupados em assumir mais obrigações contratuais (que podem afetar seus modelos de negócios) e dizem que suas ferramentas para mitigar o abuso são limitadas e podem não ser adequadas (alguns abusos podem precisar ser abordados pelos provedores de hospedagem e algumas ações dos registros e registradores podem resultar em danos colaterais e exposição a responsabilidades).

As principais iniciativas da comunidade da ICANN para resolver o abuso do DNS até agora tiveram graus variados de sucesso:

- A **Organização de Apoio para Nomes Genéricos (GNSO)** criou o Grupo de Trabalho de Políticas de Abuso de Registro em 2008. A organização identificou um conjunto de questões específicas, mas não ofereceu resultados de políticas nem realizou uma discussão subsequentes sobre práticas não vinculantes para registros e registradores (incluindo workshops durante o ICANN41 e o ICANN42).

- **Como parte do programa de novos gTLDs,** a organização da ICANN adotou uma série de novos requisitos[1] de acordo com o memorando sobre a mitigação de condutas maliciosas (3 de outubro de 2009). O relatório da ICANN sobre as proteções do Programa de Novos gTLDs (18 de julho de 2016) avaliou sua eficácia em preparação para a Revisão de concorrência, confiança e escolha do consumidor (CCT), recomendada pelo estatuto, que entregou suas recomendações em 8 de setembro de 2018.

- 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

[1] 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.

Contrato de Credenciamento de Registradores de 2013[2], 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[3].

- **Mais recentemente, a organização da ICANN,** por meio do **gabinete do diretor de tecnologia** desenvolveu a Geração de Relatórios de Atividade de Abuso de Domínios (DAAR), que oferece relatórios mensais sobre abusos e monitoramento de tendências, conforme informado mais recentemente ao GAC (24 de fevereiro de 2021). O monitoramento e a geração de relatórios sobre abuso do DNS foram apoiados ativamente pelo GAC e as equipes de revisão, que recomendaram melhorias. Espera-se que tais ferramentas aumentem a transparência e ajudem a identificar as origens dos problemas, que poderiam ser resolvidos com conformidade ou, conforme necessário, novas políticas.

Questões

As iniciativas anteriores ainda não resultaram em uma redução efetiva de abusos do DNS. Pelo contrário, está claro que ainda há muito a ser feito. Apesar da atenção da Comunidade da ICANN e as práticas recomendadas existentes no setor para mitigar o Abuso do DNS, algumas iniciativas de participação da Comunidade lideradas pelo GAC, bem como as equipes de revisão, destacaram tendências persistentes de abuso, práticas comerciais que resultam em abuso e evidências de que há um "*espaço para o desenvolvimento e o aprimoramento das atuais proteções e medidas de mitigação*", além do potencial para desenvolver políticas no futuro[4].

Além disso, as preocupações com a capacidade de mitigar com eficácia o abuso do DNS aumentaram nos círculos de aplicação da lei, segurança cibernética, proteção do consumidor e proteção intelectual[5] como consequência da entrada em vigor do Regulamento Geral de Proteção de Dados (GDPR) e das iniciativas subsequentes para mudar o sistema de WHOIS, uma ferramenta essencial para a investigação de crimes e abusos, para entrar em conformidade com o GDPR. Mais recentemente, a crise sanitária global da COVID-19 comprovou os desafios existentes, já que houve um pico de registros de domínios relacionados à pandemia.

---

[2] Consulte Recomendações das agências legais fiscalizadoras (outubro de 2019) e as 12 recomendações das agências legais fiscalizadoras (1 de março de 2012)

[3] Essas cláusulas foram complementadas por uma Estrutura não vinculante para operadores de registros responderem a ameaças à segurança (20 de outubro de 2017), aceita pela organização da ICANN, os registros e o PSWG do GAC.

[4] Consulte os comentários do GAC (19 de setembro de 2017) sobre o Relatório Final da análise estatística sobre abuso do DNS em gTLDs.

[5] Consulte a Seção III.2 e IV.2 do 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 Anti-phishing e Antiabuso de Mensagens, Malware e Dispositivos Móveis (18 de outubro de 2018)

Os Comitês Consultivos da ICANN, particularmente o GAC, o SSAC e o ALAC, e diversos terceiros afetados entraram em contato com a organização da ICANN e a comunidade da ICANN para tomar outras medidas[6].

[6] Consulte as discussões sobre abuso do DNS e Proteções do consumidor durante a cúpula de GDD (7-8 de maio de 2019)

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 geração de relatórios sobre abuso do DNS:** 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:** 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 para que possamos avançar em direção a soluções mais eficientes para a prevenção e a mitigação de abusos.

Proposta da liderança para ações do GAC

1. **Considerar as recomendações da Revisão de segurança, estabilidade e flexibilidade (SSR2)** no Relatório Final (25 de janeiro de 2021), com o **objetivo de oferecer comentários ao GAC antes da** consideração formal pela Diretoria da ICANN que deve ser feita até 25 de julho de 2021.

2. **Considerar novas contribuições para a definição de abuso do DNS** para refletir o panorama de ameaças conforme as experiências dos órgãos de aplicação da lei, em consistência com a declaração do GSC sobre abuso do DNS (18 de setembro de 2019), complementando a definição adotada pelas partes contratadas (outubro de 2020) depois do surgimento de uma Estrutura de abordagem de abusos orientada pelo setor (17 de outubro de 2019).

3. **Conversar sobre possíveis próximas etapas,** inclusive por meio de **propostas concretas para melhorar políticas e/ou cláusulas contratuais e sua aplicação**[7] para resolver questões de políticas públicas relacionadas ao abuso do DNS, conforme identificado por meio de várias iniciativas da comunidade e contribuições do GAC:

    a. **As recomendações da Revisão de CCT** de acordo com o Relatório Final (8 de setembro de 2018), considerando:

        - As ações da Diretoria da ICANN (1 de março de 2019) em relação às 35 recomendações e a subsequente adoção (26 de janeiro de 2020) de um plano de implementação proposto para as 6 recomendações aceitas (6 de setembro de 2019);
        - Comentários do GAC sobre os Comentários sobre o relatório preliminar (19 de maio de 2017), Comentários sobre a análise estatística de abuso do DNS em gTLDs (19 de setembro de 2017),
          Comentários sobre outras recomendações preliminares (15 de janeiro de 2018),
          Comentários sobre o Relatório Final da Revisão de CCT (11 de dezembro de 2018),
          Comentários sobre o plano de implementação (21 de outubro de 2019);
        - Recomendação do GAC no Comunicado de Montreal (6 de novembro de 2019) *não avançar com uma nova rodada de gTLDs antes da conclusão da implementação das recomendações da revisão de concorrência, confiança e escolha do consumidor identificadas como "pré-requisitos" ou "de alta prioridade"*.
        - Perguntas de esclarecimento da Diretoria (16 de dezembro de 2019) em relação às Recomendações do GAC em Montreal, incluindo o tema da Revisão de CCT e rodadas subsequentes de novos gTLDs e a definição de "implementação completa".

[7] De acordo com o Comunicado do GAC no ICANN69, seção IV.2: "*o GAC acredita que agora há uma expressão sólida de amplo apoio a etapas concretas a serem seguidas para abordar os principais componentes da mitigação efetiva de abusos do DNS*"; e as minutas do GAC no ICANN69: Seção 2.2 "*Pontos de ação: o PSWG do GAC deve considerar o desenvolvimento de uma proposta concreta em relação a etapas de mitigação de abusos do DNS para preparar o GAC para mais discussões no ICANN70 (de acordo com a discussão do GAC na sessão de encerramento).*"

- Resposta do GAC às perguntas de esclarecimento da Diretoria (22 de janeiro de 2020)
- Resposta da Diretoria às respostas do GAC às perguntas de esclarecimento (11 de fevereiro de 2020) em relação a sua decisão (26 de janeiro de 2020) de não aceitar nem rejeitar as recomendações.

b. **O Grupo de Trabalho do Processo de Desenvolvimento de Políticas da GNSO sobre procedimentos subsequentes de novos gTLDs** determinou em seu Relatório Final (1 de fevereiro de 2021) que "*este Grupo de Trabalho de PDP não fará recomendações com respeito à mitigação de abuso de nomes de domínio, apenas declarará que tal iniciativa futura deve valer para gTLDs novos e existentes (e possivelmente ccTLDs)*" apesar das recomendações relevantes sobre abuso do DNS enviadas pela Equipe de Revisão de CCT[8]. O GAC expressou preocupações sérias com esta decisão nos comentários do GAC (29 de setembro de 2020) sobre a versão preliminar do Relatório Final do PDG WG, bem como sua expectativa de que o Conselho da GNSO tome medidas sobre essa questão rapidamente.

c. **Implementação e aplicação das principais obrigações contratuais** em contratos de registros e registradores, especificamente:
   - **Especificação 11 do Contrato de Registro de novos gTLDs** e as recomendações de proteção relacionadas do GAC no Comunicado de Pequim (11 de abril de 2013), considerando as conclusões da auditoria de operadores de registro para abordar ameaças de segurança do DNS (17 de setembro de 2019) e discussões nas Perguntas e respostas do GAC/ICANN (30 de maio de 2017), nos Comentários do GAC no Relatório preliminar sobre CCT (19 de maio de 2017) e nos comentários do GAC sobre o relatório preliminar de SSR2 (3 de abril de 2020)
   - **A Especificação do Programa de Precisão de WHOIS** no Contrato de Credenciamento de Registradores de 2013, que inclui cláusulas sobre a verificação, a validação e a precisão de dados de registro de domínios, conforme discutido nos Comentários do GAC sobre o Relatório Final da Revisão do RDS-WHOIS2 (23 de dezembro de 2019), e o **Contato do Registrador sobre Abuso e Dever de Investigar Relatos de Abuso** (Seção 3.18), que no momento está passando por uma Auditoria de Conformidade Contratual iniciada para 153 registradores selecionados (15 de janeiro de 2021). Esses dois temas também foram discutidos nas Perguntas e respostas do GAC/ICANN (30 de maio de 2017) após as recomendações do GAC no Comunicado de Hyderabad (8 de novembro de 2016)

d. **Discussões da comunidade sobre Abuso do DNS e a eficácia das cláusulas contratuais relacionadas**, tanto em termos de aplicação quanto de viabilidade:
   - **Sessões do encontro da ICANN:** Webinar pré-ICANN66 (15 de outubro de 2019), Sessão do At-Large no ICANN66 sobre preocupações dos usuários finais (3 de

[8] Consulte a recomendação 9.15 (p. 42) do Relatório Final do WG de PDP de procedimentos subsequentes e as ações da Diretoria da ICANN relacionadas à recomendação de CCT.

novembro de 2019), Sessão entre comunidades sobre Abuso do DNS no ICANN66 (6 de novembro de 2019), Sessão do At-Large sobre conformidade contratual no ICANN67 (9 de março de 2020, Sessão do ALAC no ICANN68 sobre compromissos de interesse público e o procedimento de resolução de disputas associado (22 de junho de 2020), Reunião do Conselho da GNSO com a Diretoria no ICANN68, que discutiu possíveis próximas etapas em relação a abusos do DNS (14 de junho de 2020) e Sessão plenária do ICANN69 sobre questões de abuso do DNS (20 de outubro de 2020)

- **Correspondência entre a Diretoria da ICANN e os grupos constituintes de propriedade intelectual e negócios** da GNSO, incluindo: a declaração do BC em relação à discussão da comunidade sobre abuso do DNS (28 de outubro de 2019), uma carta do BC à Diretoria da ICANN (9 de dezembro de 2019), e a resposta subsequente (12 de fevereiro de 2020); seguida por uma carta do IPC à Diretoria da ICANN (24 de abril de 2020)

e. **Implementação de medidas antiabuso proativas pelos operadores de ccTLDs** que possam embasar as práticas de registro de gTLDs, como aquelas apresentadas pelos ccTLDs .EU e .DK.[9]

f. **As recomendações da revisão do RDS-WHOIS2,** conforme detalhadas em seu Relatório Final (8 de outubro de 2019), relevantes ao uso legítimo do WHOIS como importante ferramenta de investigação de crimes e abusos, considerando os comentários do GAC (23 de dezembro de 2019) e as ações da Diretoria da ICANN até agora (25 de fevereiro de 2020)

4. **Considerar e continuar monitorando o progresso das principais iniciativas de mitigação de abusos do DNS** na Comunidade da ICANN para embasar e promover padrões elevados em práticas e contratos:

   a. **Propostas esperadas do SSAC** para a padronização de estratégias e processos para abordar a identificação e mitigação de abusos do DNS no Relatório do Grupo de Trabalho de Abuso do DNS, que será apresentado antes do ICANN70.

   b. **Implementação de medidas voluntárias por registradores e registros de gTLDs** de acordo com a Estrutura de abordagem de abusos orientada pelo setor e discussão em andamento sobre a rede de políticas sobre Internet e jurisdição[10]

[9] Consulte especificamente uma apresentação do EURid (28 de janeiro de 2016) e uma apresentação de .DK durante o ICANN64 (12 de março de 2018)

[10] A Rede de políticas sobre internet e jurisdição recentemente anunciou (22 de fevereiro de 2021) o lançamento de um kit de ferramentas sobre ações do DNS para resolver abusos, que planeja apresentar durante uma conferência na quinta-feira, 18 de março.

c. **Melhorias na Geração de Relatórios de Atividade de Abuso de Domínios (DAAR) da ICANN** conforme discutido pelos registros com o GAC, o SSAC e o gabinete do diretor de tecnologia da ICANN[11]

d. No dia 27 de março de 2020, a organização da ICANN executou a proposta de emenda do Contrato de Registro de .COM, que estenderia as cláusulas contratuais para facilitar a detecção e a denúncia de abusos do DNS (incluindo aEspecificação 11 3b) **para dois termos do espaço de nomes de gTLDs** (até agora, ela só era aplicável a novos gTLDs). Além disso, uma carta de intenção vinculante entre a organização da ICANN e a Verisign define uma estrutura de cooperação para desenvolver práticas recomendadas e possíveis novas obrigações contratuais, além de medidas para ajudar a medir e reduzir as ameaças de segurança do DNS.

5. **Considerar os aspectos de políticas públicas do DNS sobre HTTPS (DoH)** diante dos acontecimentos recentes na implementação de tecnologias criptografadas de DNS, em consistência com as solicitações dos membros do GAC durante o ICANN69 e o trabalho em andamento do Grupo de Trabalho de Segurança Pública do GAC (PSWG) de acordo com o Plano de trabalho 2020-2021.

[11] Consulte o Relatório do Grupo de Trabalho RySG DAAR (9 de setembro de 2020), a resposta do diretor de tecnologia da ICANN (30 de setembro de 2020) e a atualização sobre o OCTO para o GAC (24 de fevereiro de 2021)

Acontecimentos relevantes

Visão geral dos acontecimentos recentes

- **Durante os encontros recentes da ICANN**, os líderes do PSWG do GAC forneceram documentos detalhados ao GAC sobre a questão do abuso do DNS (consulte o material das Sessões do GAC no ICANN66 e ICANN68, o documento do GAC sobre DNS no ICANN68, bem como a atualização do PSWG no ICANN69 para o GAC).
    - O GAC analisou as medidas disponíveis para que os registros e registradores evitem abusos do DNS, especificamente a função das políticas de registro (incluindo verificação de identidade) e estratégias de preços como determinantes importantes dos níveis de abuso em um determinado TLD.
    - O GAC também examinou iniciativas possíveis ou em andamento para resolver o abuso do DNS com mais eficácia nos níveis da Diretoria da ICANN e da organização da ICANN (consulte as Minutas do ICANN66, o Comunicado e as Minutas do GAC no ICANN68 bem como o Comunicado e as Minutas do ICANN69).
    - O Plano de Trabalho do PSWG para 2020-2021 inclui todas essas áreas dentro do objetivo estratégico 1, que é desenvolver recursos de redução de abusos do DNS e crimes cibernéticos.

- **Recomendações da Revisão de SSR2**
    - A equipe de revisão SSR2 publicou um relatório preliminar (24 de janeiro de 2020) com foco significativo em medidas para evitar e mitigar o abuso do DNS. Os comentários do GAC (3 de abril de 2020) apoiaram muitas das recomendações, especificamente aquelas relacionadas ao aprimoramento da Geração de Relatórios de Atividade de Abuso de Domínios (DAAR) e ao reforço dos mecanismos de conformidade).
    - O Relatório Final (25 de janeiro de 2021) já está aberto para comentários públicos (que terminam em abril de 2021). A estrutura do relatório foi alterada significativamente. No momento, os líderes de tópicos do GAC estão revisando o relatório e vão propor um comentário preliminar para consideração do GAC.

- **O Grupo de Trabalho sobre abuso do DNS do Comitê Consultivo de Segurança e Estabilidade (SSAC)** deve informar sobre suas atividades e conclusões antes do ICANN70.
    - Durante o encontro ICANN66, o SSAC informou ao PSWG que estava formando um Grupo de Trabalho sobre Abuso do DNS, com **a participação de um representante do PSWG**.
    - Desde então, o SSAC demonstrou sua intenção de não declarar uma definição de abuso do DNS. Em vez disso, o Grupo de Trabalho deve se concentrar nas funções das partes adequadas, com base nas perspectivas da comunidade e nas estruturas existentes. O objetivo do Grupo de Trabalho é produzir um relatório que defina possíveis iniciativas para padronizar as estratégias e os processos da comunidade em relação à identificação e mitigação de abusos.

- **Medidas e iniciativas tomadas por registros e registradores para mitigar o abuso do DNS**

- No dia 27 de março de 2020, a organização da ICANN executou a proposta de emenda do Contrato de Registro de .COM, que estenderia as cláusulas contratuais para facilitar a detecção e a denúncia de abusos do DNS (incluindo aEspecificação 11 3b) **para dois termos do espaço de nomes de gTLDs** (até agora, ela só era aplicável a novos gTLDs). Além disso, uma carta de intenção vinculante entre a organização da ICANN e a Verisign define uma estrutura de cooperação para desenvolver práticas recomendadas e possíveis novas obrigações contratuais, além de medidas para ajudar a medir e reduzir as ameaças de segurança do DNS.
- **No contexto da crise da COVID-19, as partes contratadas apresentaram suas ações e lições aprendidas** antes e durante o encontro ICANN68 enquanto as partes interessadas do PSWG relataram trabalhos contínuos em colaboração com os estados-membros da UE, Europol, ccTLDs e registradores para facilitar denúncias, análises e seu encaminhamento à jurisdição relevante por meio da adoção de um formulário padronizado para denunciar domínios/conteúdos relacionados à COVID-19 e do estabelecimento de um ponto único de contato para as autoridades relevantes. Essas iniciativas têm como base as relações de trabalho estabelecidas entre os órgãos de aplicação da lei e os registradores, além da publicação de um Guia para denúncias de abuso de registradores pelo **Grupo de interesse de registradores** durante o ICANN67.
- **Registro de Interesse Público (PIR)**, Operador de Registro de .ORG e vários novos gTLDs inauguraram (17 de fevereiro de 2021) o **Instituto de Abuso do DNS,** que declarou que seu objetivo é "*reunir líderes do espaço antiabuso para: financiar pesquisas, publicar práticas recomendadas, compartilhar dados e fornecer ferramentas para identificar e denunciar o abuso do DNS*". Essa iniciativa foi apresentada ao PSWG do GAC (3 de março de 2021) antes de um webinar que deveria ser realizado pelo Instituto em 16 de março de 2021 sobre a situação dos abusos do DNS.

- **Resposta multifacetada da organização da ICANN e execução de contratos**
  - O CEO da ICANN fez uma publicação no blog em 20 de abril de 2020 detalhando a resposta multifacetada da organização da ICANN aos abusos do DNS
  - **O gabinete do diretor de tecnologia da ICANN (OCTO) e sua equipe de segurança, estabilidade e resiliência** (SSR) conduzem pesquisas e mantêm a expertise da ICANN em segurança do DNS para o benefício da comunidade. O gabinete participa de vários fóruns de inteligência sobre ameaças cibernéticas e resposta a incidentes, incluindo o Fórum de resposta a incidentes e equipes de segurança (FIRST), o Grupo de Trabalho Antiabuso de Mensagens, Malware e Dispositivos Móveis (M3AAWG), o Grupo de Trabalho Anti-phishing (APWG), a Aliança Nacional Americana de Treinamento e Análises Forenses Cibernéticas, (NCFTA) a recente Coalizão de Ameaças Cibernéticas relacionadas à COVID-19 e a Liga de Inteligência (CTI).
    O gabinete também desenvolve sistemas e ferramentas para ajudar na identificação, análise e denúncia de abusos do DNS:
    - Diante da crise de COVID-19, o OCTO desenvolveu a ferramenta de **Coleta de informações e denúncia de ameaças de segurança de nomes de domínio**

(DNSTICR) para ajudar a identificar nomes de domínio usados para abusos relacionados à COVID-19 e compartilhar dados com as partes adequadas. O GAC recebeu informações sobre essa questão antes do ICANN68 (12 de junho de 2020), assim como a Comunidade da ICANN, durante o encontro ICANN68.

- Por meio da **Plataforma de denúncias de atividades de abuso em domínios (DAAR)**, a ICANN gerou relatórios mensais desde janeiro de 2018 sobre os registros de nomes de domínio e os comportamentos de ameaças de segurança observados no DNS. A ICANN também monitora tendências por meio dos Indicadores de integridade das tecnologias de identificadores (ITHI). Várias partes interessadas e grupos da ICANN comentaram sobre as limitações da DAAR, especificamente uma carta do M3AAWG para a organização da ICANN (5 de abril de 2019) e o relatório preliminar da equipe de revisão tSSR2 (24 de janeiro de 2020), apoiado pelo GAC (veja abaixo). O Grupo de Interesse de Registros, que também tinha manifestado preocupações em relação à DAAR e estava trabalhando com a ICANN na evolução da ferramenta, recentemente fez recomendações em uma carta para o CTO da ICANN (9 de setembro de 2020)

- O CTO da ICANN também apoia o recém-criado (6 de maio de 2020) **Grupo de Estudos Técnicos da Iniciativa de Promoção da Segurança no DNS**, como parte da implementação do Plano estratégico do AF21-25, para "*explorar ideias sobre o que a ICANN pode e deve fazer para aumentar o nível de colaboração e interação com as partes interessadas do ecossistema do DNS para melhorar o perfil de segurança do DNS*". As recomendações são esperadas para maio de 2021.
- Durante uma teleconferência do GAC sobre questões de abuso do DNS (24 de fevereiro de 2021), **a organização da ICANN deu notícias sobre as atividades da OCTO relacionadas ao abuso do DNS**, incluindo uma discussão sobre a definição de ameaças de segurança do DNS e abuso do DNS, obrigações de partes contratadas, Geração de Relatórios de Atividade de Abuso de Domínios (DAAR), Informação, Coleta e Geração de Relatórios sobre Ameaças de Segurança de Nomes de Domínio (DNSTICR), o status da Iniciativa de Facilitação de Segurança de Domínios (DSFI), a nova iniciativa de compartilhamento de conhecimento e esclarecimento de normas de segurança de nomes de domínio (KINDNS), além de uma revisão do trabalho da OCTO na área de treinamento de desenvolvimento de capacidades no mundo todo.
- **Aplicação de conformidade contratual**: em uma publicação no blog (20 de abril de 2020), o CEO da ICANN relembrou: "*A equipe de conformidade da ICANN aplica as obrigações contratuais definidas em políticas e contratos da ICANN, incluindo o Contrato de Registro (RA) e o Contrato de Credenciamento de Registradores (RAA). A equipe de conformidade da ICANN também trabalha com a OCTO para identificar ameaças de segurança no DNS [...] e associar essas ameaças às partes contratadas responsáveis. A equipe de conformidade da ICANN utiliza dados coletados em auditorias [...] para avaliar se os registros e registradores estão cumprindo suas obrigações em relação às ameaças de segurança do DNS. Além das auditorias, a equipe de conformidade da ICANN utiliza dados coletados pela OCTO e outros para interagir de forma proativa com os registros e*

registradores responsáveis por um número grande de ameaças de segurança no DNS. Quando não é possível resolver o problema por meio de interações construtivas, a equipe de conformidade da ICANN toma medidas em relação às partes que se recusam a cumprir com as obrigações relacionadas a ameaças de segurança no DNS". A publicação no blog também dava uma ideia sobre os volumes de denúncias, os recursos alocados ao processamento delas e estatísticas de resolução.

Foco: Definição de Abuso 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 contratadas com os impactos nos direitos dos usuários e nas funções básicas das partes contratadas, bem como de que a ICANN ultrapasse seu escopo.[12]

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*". [13]

O departamento de Conformidade Contratual da ICANN referiu-se a "**Abuso da infraestrutura do DNS**" e "Ameaças de 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 de segurança, como pharming, phishing, malware e botnets*"[14] — e no Contrato de Credenciamento de Registradores (Seção 3.18) — que se refere a "contatos de abuso" e "*relatórios de abuso*" sem apresentar uma definição para o termo "abuso" especificamente, mas incluindo a expressão "atividade ilegal" no escopo.

Do ponto de vista do GAC, a definição de "ameaças de segurança" incluída no Contrato de Registro de Novos gTLDs é de fato a transcrição da **definição apresentada na Recomendação 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 da ICANN a "*facilitar o trabalho da comunidade para elaborar uma definição de 'abuso' a fim de ajudar nas próximas ações para essa recomendação*"[15].

Durante um webinar antes do ICANN66 em 15 de outubro de 2019, o **PSWG e as partes contratadas discutiram as questões atuais e práticas do setor**. Em preparação para esse webinar, o Grupo de Interesse de Registros escreveu uma carta aberta (19 de agosto de 2019) explicando as opiniões dos registros sobre as definições de abuso do DNS, as opções limitadas dos registros para

---

12 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 do abuso 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.

13 Consulte a p.88 do Relatório Final da Revisão de CCT (8 de setembro de 2018) conforme destacado mais recentemente na declaração do GAC sobre abuso do DNS (18 de setembro de 2019)

14 A Especificação 11 (3)(b) do Contrato de Registro de Novos gTLDs (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*".

15 Consulte a p.5 do conjunto de indicadores de ações da Diretoria com relação às recomendações finais da equipe de CCT

tomar medidas relacionadas às ameaças de segurança e suas preocupações com a Geração de Relatórios de Atividade de Abuso de Domínios.

Em resposta, o GAC enviou uma declaração sobre abusos do DNS (18 de setembro), seguida pelo grupo constituinte de negócios (28 de outubro). Em sua declaração, o GAC reconheceu a definição da equipe de revisão de CCT de abuso do DNS como "*atividades intencionalmente enganosas, mal-intencionadas ou não solicitadas que usam ativamente o DNS e/ou os procedimentos de registro nomes de domínio*" que, em termos técnicos podem assumir a forma de ameaças de segurança, como "*malware, phishing e botnets, e também spam, quando usado como método de distribuição dessas formas de abuso*". O GAC reconheceu que o Contrato de Registro de novos gTLDs reflete essa ideia na Especificação 11, especialmente nas seções 3a[16] e 3b[17].

Depois da publicação da Declaração do GAC sobre abuso do DNS (18 de setembro de 2019), um grupo de **grandes registros e registradores de gTLDs propôs uma** estrutura voluntária para reduzir os abusos (17 de outubro de 2019). Especificamente, essa estrutura inclui na cobertura de possíveis medidas pelos adotantes certas formas de "abuso de conteúdos de sites", consideradas "tão graves que a parte contratada deve tomar medidas diante de uma notificação específica e confiável". Depois da publicação e discussão durante o ICANN66, a lista de signatários dessa estrutura aumentou, incluindo outros grandes registradores e registros, além de pequenos provedores desse tipo de serviço.

Em 18 de junho de 2020, os presidentes dos Grupos de partes interessadas de registros e registradores (coletivamente chamados de Casa das Partes Contratadas da GNSO ou CPH) informaram aos líderes da comunidade que adotaram uma definição de abuso do DNS refletindo exatamente aquela da estrutura criada pelo setor para reduzir os abusos:

> *O abuso do DNS é composto por cinco categorias mais amplas de atividades nocivas na medida em que se relacionam ao DNS: malware, botnets, phishing, pharming e spam como mecanismo de distribuição de outras formas de abuso do DNS* [fazendo referência ao documento de abordagens operacionais, normas, critérios e mecanismos da Rede de Políticas de Internet e Jurisdição para a definição de cada uma dessas atividades].

Essa definição **parece confirmar o que a equipe de revisão de CCT chamou de consenso existente em relação ao** "**Abuso de segurança do DNS** ou Abuso de segurança do DNS na infraestrutura do DNS" (Relatório Final de CCT p. 8.) e **concorda com a definição ilustrativa do GAC de** "**ameaças de segurança**" nas 'verificações de segurança' das recomendações de proteção do GAC válidas para

[16] A Especificação 11 3a determina que "O operador de registro incluirá uma cláusula em seu contrato entre registro e registrador que exija que os registradores *coloquem em seus contratos de registro uma cláusula que proíba os titulares de nome registrado de distribuir malware, botnets que operem de forma abusiva, phishing, pirataria, violação de marca comercial ou de direitos autorais, práticas fraudulentas ou enganosas, falsificações ou, de outra forma, se envolver em atividades contrárias à legislação aplicável e gerar (de acordo com a legislação aplicável e qualquer procedimento relacionado) consequências para tais atividades, inclusive a suspensão do nome de domínio*".

[17] Já a Especificação 11 3b determina que "O Operador de registro realizará periodicamente uma análise técnica para avaliar se os domínios no TLD estão sendo usados para cometer ameaças de segurança, como pharming, phishing, malware e botnets. *O Operador de registro manterá relatórios estatísticos sobre o número de ameaças de segurança identificadas e as ações tomadas como resultado das verificações de segurança periódicas. O Operador de registro manterá esses relatórios pelo período do Contrato, a menos que um período mais curto seja exigido por lei ou aprovado pela ICANN, e os fornecerá à ICANN mediante solicitação.*"

todos os novos gTLDs no Comunicado de Pequim (11 de abril de 2013), incorporadas ao Contrato de Registro de gTLDs na Especificação 11 3.b.

Foco: 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 (17 de setembro de 2013) foi aprovado pela Diretoria da ICANN (27 de junho de 2013) após a inclusão das cláusulas sobre as 12 recomendações das agências legais fiscalizadoras (1 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 das cláusulas em linha com as recomendações de proteções do GAC no Comunicado de Pequim (11 de abril de 2013), em consistência com a Proposta da Diretoria da ICANN para a 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 temas de interesse do GAC pendentes, uma recomendação sobre a Especificação 11 (3)(b) do Contrato de Registro de Novos gTLDs foi publicada em 8 de junho de 2017 em resposta a perguntas de alguns operadores de registro em busca de orientações sobre como garantir a conformidade com a Seção 3b da Especificação 11 (3)(b) do Contrato de Registro de Novos gTLDs. **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*".[18] 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*

[18] Conforme relatado na publicação em 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

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 assumiu o compromisso de abordar as ameaças de segurança do DNS.
- A prevalência de ameaças de segurança se concentra em um número relativamente pequeno de operadores de registro.
- Alguns operadores de registro interpretam o texto contratual da Especificação 11 3(b) de uma forma que dificulta definir se o trabalho de mitigação de ameaças de segurança do DNS é efetivo e está em conformidade.

As **partes contratadas consideram que os problemas com essas auditorias** excede o escopo das suas obrigações contratuais.[19] A organização da ICANN indicou que iniciará uma auditoria dos registradores com foco nas ameaças de segurança do DNS.

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

Como parte do Programa de Novos gTLDs, a Diretoria da ICANN resolveu (25 de junho de 2013) incluir as chamadas "verificações de segurança" (Conselho de Proteções do GAC no 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 Diretoria 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 formou uma equipe de redação composta por voluntários de Registros, Registradores e do GAC (incluindo membros do PSWG), que desenvolveram a Estrutura para operadores de registros responderem a ameaças à segurança publicada em 20 de outubro de 2017, depois de passar por 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 um "*órgão nacional de aplicação das leis ou agência de segurança pública de uma jurisdição apropriada*".

[19] Consulte a correspondência do RySG (2 de novembro de 2019) à qual a organização da ICANN respondeu (8 de novembro), e os comentários publicados na página do comunicado (15 de novembro): os registros consideraram problemáticas as questões de auditoria, que ameaçam a aplicação de medidas fora do escopo de suas obrigações contratuais [especificamente aEspecificação 11 3b] e indicaram relutância em "*compartilhar com a organização da ICANN e a comunidade informações relevantes sobre o trabalho contínuo para combater o abuso do DNS [...] como parte de uma iniciativa de conformidade da ICANN que vai além do permitido dentro do Contrato de Registro*"

De acordo com a recomendação 19, a Equipe de revisão de CCT adiou a tarefa de conduzir uma avaliação da eficácia da estrutura para uma revisão subsequente[20], já que a estrutura não existe há tempo suficiente para avaliar sua eficácia.

[20] 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.*

Foco: Consideração das recomendações da Revisão de CCT sobre Abuso de DNS

Com base em sua análise do panorama de abusos do DNS,[21] 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 abuso do DNS (9 de agosto de 2017), a equipe de revisão de CCT recomendou, em relação ao abuso 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)

A Diretoria da ICANN resolveu (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*".[22]

Diante das recomendações no Comunicado do GAC de Montreal (6 de novembro de 2019) de que a Diretoria da ICANN "*não faça uma nova rodada de gTLDs antes de concluir a implementação das recomendações [...] identificadas como "pré-requisitos" ou de "alta prioridade*", e da resposta da Diretoria a essas recomendações (26 de janeiro de 2020), o PSWG continua monitorando a consideração das principais recomendações da CCT-RT (6 de setembro de 2018) voltadas para a adoção de cláusulas contratuais para incentivas medidas proativas antiabuso (Rec. 14) e para evitar o uso sistêmico de registradores ou registros para abuso do DNS (Rec. 15); o aprimoramento das pesquisas sobre abuso do DNS (Rec. 16); o aprimoramento da precisão do WHOIS (Rec. 18); e a eficácia do processamento de denúncias de conformidade contratual (Rec. 20).

O PSWG do GAC também está considerando a resolução da Diretoria de continuar com o plano de implementação da ICANN (23 de agosto de 2019) para recomendações de CCT aceitas no Conjunto de indicadores de ações da Diretoria (1 de março de 2019). O GAC comentou (21 de outubro de 2019) sobre esse plano e destacou alguns pontos problemáticos com relação às importantes recomendações de combater o abuso do DNS, incluindo a publicação da cadeia de partes responsáveis pelos registros de nomes de domínio de gTLDs (Rec. 17), informações mais detalhadas sobre denúncias de conformidade contratual (Rec. 21), medidas de segurança proporcionais à oferta de serviços que envolvem a coleta de informações confidenciais de saúde e financeiras (Rec. 22).

Depois da adoção pelas partes contratadas de uma definição de abuso de DNS, o **GAC pediu esclarecimentos à Diretoria da ICANN durante o ICANN68** (veja o material das reuniões do GAC

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

[22] Consulte a p.5 do conjunto de indicadores de ações da Diretoria com relação às recomendações finais da equipe de CCT

com a Diretoria em 24 de junho de 2020), em relação à implementação da Rec. 14 da CCT-RT (a *ICANN deveria negociar cláusulas contratuais para fornecer incentivos financeiros às partes contratadas para a adoção de medidas proativas antiabuso*), perguntando o status e o planejamento para a condução de iniciativas da comunidade para desenvolver uma definição de "abuso" e embasar outras ações da Diretoria em relação a essa recomendação. O GAC registrou em suas Minutas do ICANN68 que "*a Diretoria continuará promovendo o diálogo da comunidade como já vem fazendo, conduzindo discussões regionais e entre comunidades, fazendo pesquisas e desenvolvendo ferramentas para ajudar a embasar os debates da comunidade, além de enviar palestrantes quando solicitado*".

Durante o encontro ICANN68, o PSWG observou com as partes interessadas do ALAC que o progresso na implementação da recomendação da CCT-RT aceita e a consideração das recomendações pendentes não estão claros. Também ficou clara a insatisfação com um comunicado (29 de abril de 2020) do **Grupo de Trabalho do Processo de Desenvolvimento de Políticas da GNSO para Procedimentos Subsequentes de Novos gTLDs,** dizendo que "*não planeja fazer recomendações em relação à redução do abuso de nomes de domínio, apenas dizer que tais iniciativas devem ser aplicadas tanto aos gTLDs existentes quanto aos novos (e possivelmente aos ccTLDs)*". Esse comentário foi feito mesmo com as recomendações relevantes feitas pela equipe de revisão de CCT, apoiadas por ações da Diretoria da ICANN a esse respeito, além das Recomendações do comunicado do GAC de Montreal (6 de novembro de 2019) e dos comentários do GAC registrados no Comunicado do GAC no ICANN67 (16 de março de 2020)

Em seu Relatório Final (1 de fevereiro de 2021), o Grupo de Trabalho do Processo de Desenvolvimento de Políticas da GNSO sobre Procedimentos Subsequentes de Novos gTLDs confirmou sua decisão[23]. O GAC expressou preocupações sérias com essa questão nos comentários do GAC (29 de setembro de 2020) sobre a versão preliminar do Relatório Final do PDG WG, bem como sua expectativa de que o Conselho da GNSO tome medidas sobre essa questão rapidamente.

Foco: Discussão de desenvolvimentos de políticas da GNSO sobre mitigação de abusos do DNS

Depois da decisão inicial do Grupo de Trabalho do PDP de Procedimentos Subsequentes de Novos gTLDs de não fazer recomendações em relação ao abuso do DNS para futuros contratos de novos gTLDs, o **Conselho da GNSO discutiu** em uma reunião realizada em 21 de março de 2020 **a possibilidade de iniciar um Grupo de Trabalho Entre Comunidades (CCWG)** sobre questões relacionadas ao abuso do DNS e possivelmente um subsequente PDP da GNSO, caso fossem necessários novos requisitos contratuais.

O Conselho não discutiu uma proposta informal da liderança do GAC (12 de maio de 2020) de considerar uma discussão entre especialistas relevantes, incluindo operadores de ccTLDs, sobre futuras iniciativas de políticas.

[23] Consulte o Relatório Final do WG de PDP de procedimentos subsequentes, recomendação 9.15 (p. 42)

Em 18 de fevereiro de 2021, essa questão continuava identificada como “não planejada” no Radar de decisões e ações do Conselho da GNSO, e o Conselho da GNSO deve “determinar as próximas etapas, se for o caso, em relação ao abuso do DNS”. A liderança do GAC e os líderes de temas relevantes devem discutir essa questão em uma teleconferência entre o GAC e a GNSO antes do ICANN70 (8 de março de 2021), em preparação para a reunião do GAC com a GNSO no ICANN70 (24 de março de 2021).

Foco: 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 da 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).[24]

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*". A partir de janeiro de 2018, isso é feito por meio da publicação de relatórios mensais, com base na compilação de dados de registro de TLDs com informações de um amplo conjunto de feeds de dados de alta confiança sobre ameaças à segurança e reputação.[25]

Dessa forma, o DAAR está contribuindo para o requisito identificado pelo GAC de publicar "*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[26] para a organização da 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 dos membros do PSWG do GAC e dos parceiros de segurança cibernética de fornecer informações para ações viáveis.

Recentemente, os registros informaram em uma carta aberta (19 de agosto de 2019) que interagiram com o gabinete do diretor de tecnologia "*para analisar o DAAR em busca de recomendar aprimoramentos à OCTO a fim de garantir que o DAAR cumpre melhor sua finalidade e seja um recurso valioso para a comunidade da ICANN*". Embora os registros tenham reconhecido que "*alguns membros da comunidade podem não confiar nos dados fornecidos pela Geração de Relatórios de Atividade de Abuso de Domínios da ICANN (ou DAAR) para embasar alegações de abuso sistêmico ou prevalente do DNS*", eles acreditam que "*a ferramenta tem limitações significativas, não é confiável para fornecer evidências precisas de ameaças de segurança e ainda não cumpre seus objetivos*".

O Grupo de Interesse de Registros falou sobre seu trabalho no Relatório do Grupo de Trabalho do DAAR (9 de setembro de 2020), em resposta ao qual o diretor de tecnologia da ICANN afirmou (30 de setembro de 2020): "*a maioria das recomendações da carta destaca a melhoria da comunicação sobre os dados exportados do sistema DAAR, já que essa comunicação é considerada possivelmente confusa pelo Grupo de Trabalho, tanto em relação à documentação da metodologia atual do DAAR quanto nos relatórios mensais do DAAR. Embora muitas das recomendações se concentrem em alterações específicas ao relatório, algumas (como a recomendação 3, que pede a*

[24] Consulte as sessões entre comunidades lideradas pelo PSWG do GAC durante o ICANN57 (novembro de 2016), ICANN58 (março de 2017) e ICANN60 (outubro de 2017), bem como as perguntas à Diretoria da ICANN em relação à eficácia das Proteções contra abusos do DNS no Comunicado de Hyderabad (8 de novembro de 2016), perguntas adicionais do Comunicado do GAC de Copenhague (15 de março de 2017) e um conjunto de respostas preliminares (30 de maio de 2017) elaboradas pela organização da ICANN.

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

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

medição da "persistência" das atividades abusivas informadas) podem exigir investigação e análise em mais longo prazo."

Durante a atualização da OCTO para o GAC (24 de fevereiro de 2021), o diretor de tecnologia da ICANN discutiu futuros planos para o desenvolvimento do DAAR: adicionar mais ccTLDs ao escopo do DAAR, continuar trabalhando com o Grupo de Trabalho do DAAR RySG, e explorar soluções para superar os desafios no acesso aos dados de WHOIS para desenvolver métricas em nível de registrador, incluindo consultas diárias ao WHOIS apenas para domínios em listas de proibições, amostras aleatórias de domínios ou a busca de aprovação para usar dados de Acesso a Dados de Registro em Lote (BRDA).

Posições atuais

As posições atuais do GAC estão indicadas abaixo em ordem cronológica reversa:

- Comunicado do GAC no ICANN69 (23 de outubro de 2020) observando que o GAC acredita que "*agora há uma expressão sólida de amplo apoio às medidas concretas a tomar para abordar os principais componentes da mitigação efetiva de abusos do DNS*" diante do aumento do impulso do diálogo construtivo na Comunidade da ICANN (consulte a seção IV.2 p.6).
- Comunicado do GAC no ICANN68 (27 de junho de 2020) observando que "as *novas iniciativas para reduzir o abuso do DNS não devem substituir, mas sim complementar as iniciativas existentes para melhorar a precisão dos dados de registro, como o Sistema de Geração de Relatórios de Precisão, além da implementação de políticas sobre serviços de privacidade e proxy, que no momento estão suspensas*" (consulte a seção IV.3 p.7)
- Comentários do GAC (3 de abril de 2020) sobre o Relatório Preliminar da Equipe de revisão SSR2
- Comentários do GAC sobre as recomendações finais da revisão do RDS-WHOIS2 (23 de dezembro de 2019)
- Declaração do GAC sobre abuso do DNS (18 de setembro de 2019)
- Comentários do GAC sobre o relatório final da equipe de revisão de CCT (11 de dezembro de 2018)
- Comentários 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)
- Comentários do GAC sobre a análise estatística de abuso do DNS em gTLDs (19 de setembro de 2017)
- Comentários do GAC sobre o Relatório das Proteções do Programa de Novos gTLDs contra o Abuso do DNS (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 (p. 3) e IV.2 Legislação sobre Proteção de Dados e WHOIS (p.
- Comunicado do GAC de Copenhague (15 de março de 2017) inclusive a Recomendação de Mitigação de Abusos solicitando respostas para o conjunto de indicadores de

acompanhamento do GAC relacionado ao Anexo 1 do Comunicado do GAC de Hyderabad (pp. 11 a 32)

- Comunicado do GAC de Hyderabad (8 de novembro de 2016) inclusive a Recomendação de Mitigação de Abuso 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 2011), seção VI. recomendações de devida diligência das agências legais fiscalizadoras
- Recomendações de LEAs sobre aditamentos aos Contratos de Registros (1 de março de 2012)
- Recomendações de auditoria de cumprimento da lei (Out. 2009)

Principais documentos de referência

- Documentação do GAC sobre abuso do DNS
    - Documento do GAC sobre abuso do DNS no ICANN68 (18 de junho de 2020)
    - Perguntas do GAC sobre a mitigação de abusos e respostas preliminares da ICANN (30 de maio de 2017) de acordo com as recomendações no Comunicado do GAC de Hyderabad (8 de novembro de 2016) e acompanhamento no Comunicado do GAC de Copenhague (15 de março de 2017)
- Definição de Abuso do DNS (incluindo a perspectiva das partes interessadas do setor)
    - Definição de Abuso do DNS segundo as partes contratadas (outubro de 2020)
    - Estrutura para abordar o abuso do DNS (17 de outubro de 2019)
    - Declaração do GAC sobre abuso do DNS (18 de setembro de 2019)
- Revisão SSR2 - Relatório Final (25 de janeiro de 2021
- Segunda revisão do RDS-WHOIS
    - Conjunto de indicadores de ações da Diretoria da ICANN (25 de fevereiro de 2020) sobre as recomendações finais da Revisão do RDS-WHOIS
    - Recomendações finais da Revisão do RDS-WHOIS2 (3 de setembro de 2019)
- Revisão de concorrência, confiança e escolha do consumidor
    - Relatório Final e Recomendações da Revisão de CCT (8 de setembro 2018), especificamente a seção 9 das Proteções (p.88)
    - Conjunto de indicadores de ações da Diretoria da ICANN em relação às recomendações finais da equipe de CCT (1 de março de 2019)
    - Análise estatística de abuso do DNS em gTLDs (9 de agosto de 2017)

Administração do documento

Encontro	Fórum Virtual da Comunidade ICANN70, de 22 a 25 de março de 2021
Título	Mitigação de abusos do DNS
Distribuição	Membros do GAC (antes do encontro) e público (depois do encontro)
Data de distribuição	Versão 1: 11 de março de 2021