ICANN | GAC

Governmental Advisory Committee

Distribuição	Comentários
Data	18 de setembro de 2019

Declaração do GAC sobre abuso do DNS

O Comitê Consultivo para Assuntos Governamentais (GAC) da ICANN espera a próxima discussão entre comunidades sobre abusos do DNS durante o ICANN66 e reconhece a carta aberta do Grupo de Interesse de Registros sobre o assunto, enviada à comunidade em 19 de agosto de 2019.

Proteger o público contra ameaças de segurança e abuso do DNS é uma questão de políticas públicas muito importante. O GAC apresentou recomendações, orientações e comentários, organizou discussões entre comunidades e defendeu cláusulas contratuais mais robustas para proteger o público. [1] Nossas observações atuais darão mais contexto sobre o tema, com a discussão de: 1) por que o abuso do DNS é um tema essencial; 2) as definições existentes e obrigações contratuais em relação a abusos do DNS; e 3) as conclusões da Equipe de Revisão de Concorrência, Confiança e Escolha do Consumidor e suas recomendações sobre abuso do DNS. Com essa discussão, esperamos estabelecer a base para uma discussão produtiva e embasada entre comunidades em Montreal.

Por que o abuso do DNS é um tema essencial

A cada ano que passa, o custo global dos crimes cibernéticos aumenta, chegando a uma estimativa de US$ 600 Bi[2] Os criminosos cibernéticos exploram e abusam do DNS para fazer suas tramoias,[3] e o e-mail continua sendo o vetor mais comum para a invasão inicial,[4] com um grande aumento dos ataques de phishing contra os consumidores.[5]

Para que o público confie na Internet para comunicações e transações, as pessoas encarregadas de administrar a infraestrutura do DNS devem tomar medidas para garantir que esse recurso público seja seguro e protegido. As leis recentes de privacidade, incluindo o Regulamento Geral de Proteção de Dados da UE, limitaram a disponibilidade pública de informações sobre os proprietários de nomes de domínio, gerando desafios para os profissionais de aplicação da lei e segurança cibernética encarregados de combater ameaças à proteção e à segurança da Internet.[6]

---

1 O GAC fez esses comentários de forma independente e por meio do Grupo de Trabalho de Segurança Pública. Consulte, por exemplo, o seguinte: Comunicados do GAC: ICANN46 Pequim; ICANN 53 Buenos Aires, ICANN54 Dublin; e ICANN57 Hyderabad; apresentações da comunidade da ICANN sobre abuso do DNS no ICANN57, 58 e 60; e recomendações de aplicação da lei de 2009 (apoiadas pelo GAC durante o ICANN 38).

2 McAfee Economic Impact of Cybercrime – No Slowing Down, disponível em: ;https://www.csis.org/analysis/economic-impact-cybercrime Accenture 2019 Cost of Cybercrime, disponível em: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

3 *Consulte, por exemplo, o relatório de segurança e ameaças na Internet da* Symantec (fevereiro de 2019), disponível em: .https://www.symantec.com/security-center/threat-report

4 Relatório de investigações de violações de dados da Verizon, 2019, disponível em: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations- report.pdf

5 Akamai's 2019 State of the Internet, disponível em https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial- services-attack-economy-report-2019.pdf

6 *Consulte, por exemplo,* a pesquisa sobre GDPR da ICANN com usuários do WHOIS, conduzida pelo Grupo de Trabalho Anti-phishing e pelo Grupo de Trabalho antiabuso e malware em mensagens e dispositivos móveis, disponível em lhttps://www.securityskeptic.com/2019/03/facts-figures-whois-policy-changes-impair-blacklisting-defenses.htm

As revisões recentes e contínuas da ICANN, exigidas pelo Estatuto, destacam a importância do seguinte:

- a **eficácia do trabalho de segurança para lidar com desafios e ameaças reais e potenciais à segurança e estabilidade do DNS**, e em que medida as **iniciativas de segurança são robustas o suficiente para encarar futuros desafios** e ameaças;[7]
- **proteção do consumidor**, segurança, estabilidade e resiliência, problemas de **violações mal-intencionadas**, questões de soberania e proteção de direitos antes ou depois do aumento do número de autorizações de novos domínios de primeiro nível;[8]
- **melhorar a precisão e o acesso a dados de registro de domínios genéricos de primeiro nível**, além de considerar proteções para tais dados;[9]
- a **eficácia** do **serviço de diretório de registro de gTLDs atual** e se a **implementação dele atende às necessidades legítimas dos órgãos de fiscalização, promovendo a confiança** do consumidor e protegendo os dados dos registrantes[10] [destaques adicionados]

Além disso, a ICANN está considerando a estrutura de uma segunda rodada de gTLDs, oferecendo novas oportunidades de incluir nos contratos incentivos para a adoção de práticas recomendadas que comprovadamente reduzem esses abusos e aumentam as penalidades para criminosos ou invasores.

Por isso, agora é o momento certo de considerar essas questões e contemplar o melhor caminho a seguir para promover o compromisso da ICANN de preservar e **aprimorar** a administração do DNS, incluindo a "estabilidade operacional, confiabilidade, segurança, interoperabilidade global, resiliência e abertura do DNS e da Internet."[11]
Com relação a isso, os governos e as autoridades públicas estão em uma boa posição para opinar.[12]

Definições existentes de abuso do DNS e obrigações contratuais da ICANN

A equipe de revisão de concorrência, confiança e escolha do consumidor (CCT), formada por partes interessadas da comunidade da ICANN, analisou as definições existentes de abuso do DNS na comunidade da ICANN, buscando comparar o abuso do DNS em novos gTLDs e em gTLDs antigos, além de avaliar se as proteções existentes são suficientes.[13] Observando que as conclusões da comunidade da ICANN demonstram que "existe um consenso em relação ao que constitui abuso de segurança do DNS ou abuso de infraestrutura do DNS", a **equipe de revisão de CCT passou a referir-se a abuso de DNS como "atividades intencionalmente enganosas, conspirativas ou não solicitadas que fazem uso ativo do DNS e/ou de outros procedimentos usados para registrar nomes de domínio**".[14] O Relatório da CCT usou o termo "abuso de segurança do DNS" para se referir a formas mais técnicas de atividade mal-intencionada, como malware, phishing e botnets, além de spam, quando usadas como método de distribuição dessas formas de abuso.[15]

---

7 Estatuto da ICANN, §4.6 (c), Revisão de Segurança, Estabilidade e Resiliência.
8 Estatuto da ICANN, §4.6 (d), Revisão de Concorrência, confiança e escolha do consumidor.
9 Estatuto da ICANN, §4.6 (e), Revisão de Serviços de Diretório de Registro.
10 *Id.*
11 Estatuto da ICANN, §1.2(a) Compromissos.
12 Reconhecer a função essencial dos governos e autoridades públicas em contribuir para questões de políticas públicas é um dos valores essenciais da ICANN. Estatuto da ICANN, §1.2(b) Valores essenciais.
13 Consulte o relatório final da CCT (18 de setembro de 2018), páginas. 88-109. Para saber mais sobre como o abuso foi caracterizado pela Comunidade da ICANN, consulte o Relatório Final do Grupo de Trabalho de Políticas de Abuso de Registros (29 de maio de 2010): https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf
14 Relatório Final da CCT, página 88 e conclusões. Consulte também a página 3 das "Proteções do Programa de Novos gTLDs contra abuso do DNS: Relatório Revisado" (2016)
15 Relatório Final da CCT, página 8

Essas definições são consistentes com os contratos padrão da ICANN para registros e registradores. O Contrato de Registro padrão da ICANN exige que os operadores de registro de novos gTLDs incluam cláusulas em seus contratos entre registros e registradores (RRA) que proíbam os registrantes de:

> distribuir malware, botnets que operam de modo abusivo, phishing, pirataria, violação de marca registrada ou de direitos autorais, práticas fraudulentas ou enganosas, falsificação ou outro tipo de envolvimento 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.[16]

Além disso, os operadores de registro devem "realizar periodicamente uma análise técnica para avaliar se os domínios no TLD estão sendo usados para espalhar ameaças de segurança, **como** pharming, phishing, malware e botnets".[17] [destaque adicionado]. Vale lembrar que essa lista é ilustrativa, não inclui todas as possibilidades. Complementando as cláusulas para os registros, o contrato padrão da ICANN para registradores exige que eles "investiguem rapidamente qualquer denúncia de abuso e respondam de forma adequada".[18] Juntas, essas definições desenvolvidas pela comunidade multissetorial da ICANN formam uma noção básica do que constitui abuso do DNS.

Equipe de revisão de CCT conclui que o abuso do DNS está concentrado entre certos registros e registradores e desenvolve recomendações

A equipe de CCT observou que os nomes de domínio costumam ser um componente importante dos crimes cibernéticos, são usados para ajudar na distribuição de malware e comandos e controles de botnets, e que as campanhas de spam costumam estar correlacionadas a phishing e outros crimes cibernéticos.[19] Particularmente, a equipe de revisão destacou que

> embora os contratos padrão da ICANN para registros e registradores solicitem o uso consistente das proteções especificadas, o trabalho para combater o abuso de nomes de domínio varia imensamente entre as partes contratadas. Algumas entidades só tomam medidas quando recebem denúncias. Por outro lado, outros registradores tomam medidas proativas, como verificar as credenciais dos registrantes, bloquear cadeias de caracteres de nomes de domínio similares a alvos de phishing conhecidos e inspecionar os revendedores de nomes de domínio. Os revendedores de nomes de domínio não são partes contratadas da ICANN, portanto não estão diretamente sujeitos à autoridade da ICANN pelos requisitos dos contratos padrão. . . [20]

Para entender melhor a eficácia das proteções de novos gTLDs, a equipe de revisão de CCT encomendou um estudo para analisar os índices de distribuição de spam, phishing e malware nos gTLDs globais de 2014 a 2016, diferenciando entre gTLDs antigos e novos, e posteriormente apresentou um relatório.[21]

---

[16] Contrato de Registro da ICANN, Especificação 11, 3(a).

[17] Contrato de Registro da ICANN, Especificação 11, 3(b). Esta cláusula foi tema de várias perguntas, preocupações e recomendações do GAC, que surgiram por causa da implementação dessa proteção pela ICANN, que passou a exigir que os registros monitorassem ameaças de segurança, mas não obriga os operadores de registro a tomar medidas para responder a ameaças de segurança. Consulte Cingapura (2014), Los Angeles, Londres. O Comunicado do GAC de Pequim incluía não só o dever de monitorar ameaças de segurança, mas também o dever de responder em caso de detecção de certas ameaças de segurança. O GAC recomendou que, "no caso de ameaças de segurança que representem um risco real, os operadores de registro deverão informar o registrador pertinente e, se ele não tomar medidas imediatas, suspender o nome de domínio até que o problema seja resolvido". Comunicado de Pequim, página 7.

[18] Contrato de Registrador da ICANN, § 3.18.

[19] Relatório Final da Equipe de CCT, página 93.

[20] Relatório Final da Equipe de CCT, página 93.

[21] *Consulte* https://www.icann.org/news/announcement-2017-08-09-en

O estudo sobre abuso do DNS deixa claro que existem problemas significativos de abusos no DNS. Em relação ao programa de novos gTLDs, o estudo observa que mais de 50% dos registros em certos novos gTLDs foram abusivos.[22] Outros destaques do estudo são:

- Os novos gTLDs são um alvo cada vez maior para os invasores;
- Os gTLDs antigos têm maior concentração de domínios comprometidos, mas os invasores costumam escolher novos gTLDs para registrar nomes de domínio mal-intencionados;
- Os operadores de registro dos novos gTLDs que mais sofrem abusos competem com o preço;
- Os índices de abusos por phishing e malware em novos gTLDs estão se aproximando aos índices dos gTLDs antigos com o tempo;
- Os cinco novos gTLDs com a maior concentração de domínios usados em ataques de phishing, de acordo com a lista negra do Grupo de Trabalho Anti-Phishing, continham 58,7% de todos os domínios colocados em lista negra entre os novos gTLDs;
- No último trimestre de 2016, os novos gTLDs tiveram uma porcentagem significativamente mais alta de spam do que os gTLDs mais antigos (dez vezes maior);
- Os nomes de domínio registrados para fins mal-intencionados costumam conter cadeias de caracteres relacionadas a termos que são marcas comerciais
- O número de abusos tem correlação com requisitos estritos para o registro: ou seja, os invasores preferem registrar domínios em novos gTLDs padrão, que costumam ser abertos para registro público, em vez de usar novos gTLDs da comunidade, em que os registros podem impor restrições sobre quem ou quais entidades podem registrar os nomes de domínio.

A Equipe de revisão de CCT concluiu que fatores como restrições de registro, preço e práticas específicas do registrador podem afetar os índices de abuso.[23] Por consequência, a equipe de revisão de CCT recomendou que:

- A organização da ICANN negocie emendas aos Contratos de Registro existentes ou, no caso de novos Contratos de Registro associados a rodadas subsequentes de novos gTLDs, **inclua cláusulas nos contratos para oferecer incentivos, incluindo financeiros, para os registros, especialmente registros abertos, que adotem medidas proativas de combate ao abuso** [destaque adicionado];
- A organização da ICANN negocie emendas ao Contrato de Credenciamento de Registradores e ao Contrato de Registro para incluir cláusulas que evitem o uso sistêmico de registradores ou registros específicos para o abuso de segurança do DNS. Especificamente, a ICANN deve estabelecer limites de abuso para o acionamento automático de investigações de conformidade, além de um limite mais alto para considerar automaticamente que os registradores e registros não estão cumprindo seus contratos;
- É necessário estudar melhor a relação entre operadores de registro e registradores específicos e abuso de segurança do DNS, com coleta de dados contínua, incluindo, entre outros, a iniciativa de denúncias de atividades abusivas em domínios (DAAR) da ICANN. Para fins de transparência, essas informações devem ser publicadas regularmente, o ideal seria a cada trimestre ou no mínimo uma vez por ano, para permitir a identificação de registros e registradores que precisam de mais análise, investigação e possíveis medidas da organização da ICANN. Depois de identificar o fenômeno do abuso, a ICANN deve colocar em prática um plano de ação para responder a esses estudos, corrigir os problemas identificados e definir a futura coleta de dados constante; e
- A ICANN deve reunir dados sobre a cadeia de responsáveis pelo registro de nomes de domínios de gTLDs e publicar essas informações.

[22] Relatório Final da análise estatística de abusos do DNS em gTLDs (9 de agosto de 2017): https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf
[23] Relatório Final da CCT, página 94, citando o estudo sobre abuso do DNS, pp. 24-25.

Práticas recomendadas para registros de ccTLDs

Nos últimos anos, um número cada vez maior de registros de ccTLDs adotaram medidas proativas antiabuso para combater crimes realizados via DNS, mantendo suas zonas livres de abuso e expulsando os invasores, fazendo com que seus nomes de domínio sejam cada vez menos atrativos para pessoas mal-intencionadas. Essas medidas vão de métodos de autenticação mais robustos, como verificação de identidade, [24] ao uso de modelos de previsão de fraude baseados em dados, que combinam métricas de registro de dados e infraestrutura para identificar e prever os registros de domínio mal-intencionados. [25] Essas práticas recomendadas comprovadas devem ser implementadas pelos registros e registradores de gTLDs.

Conclusão

Esta comunidade é a mais indicada para avaliar e escolher as políticas que devem ser adotadas para proteger o público contra o abuso do DNS. Concordamos com o grupo de Interesse de Registros que o sucesso deles (e do DNS) depende da capacidade de oferecer um produto respeitável, em que os usuários possam confiar. Para atacar com mais eficiência o abuso do DNS e aumentar a confiabilidade do sistema, recomendamos que a Comunidade considere seriamente a adoção das recomendações descritas acima, que oferecem medidas práticas que podem e devem ser seguidas para combater o abuso do DNS. O GAC espera conversar com outros grupos da comunidade sobre esse assunto no ICANN66 em Montreal.

[24] Consulte, por exemplo, a Sessão:sobre lições aprendidas no ICANN64: Como .DK conseguiu reduzir os domínios abusivos e https://www.dk.hostmaster.dk/en/news/mandatory- identification-nemid e https://www.dk-hostmaster.dk/en/news/dk-hostmaster-makes-online-fraud-more-difficult

[25] Consulte https://eurid.eu/en/news/identification-of-malicious-dns/