ICANN | GAC
Governmental Advisory Committee

发布	公众
日期	2019 年 9 月 18 日

关于 DNS 滥用的 GAC 声明

ICANN 政府咨询委员会 (GAC) 期待在 ICANN66 会议期间开展新一轮 DNS 滥用跨社群讨论，感谢注册管理机构利益相关方团体于 2019 年 8 月 19 日就这一主题发布的社群公开信函。

保护公众安全、缓解安全威胁和打击 DNS 滥用是一项重要的公共政策课题。GAC 广泛发表意见，提供指导和意见，组织跨社群讨论，呼吁强化合同条款，积极维护公众利益。[1] 我们就以下方面开展讨论并广泛征询意见，为探讨本主题进一步奠定基础：1) 为什么 DNS 滥用主题至关重要；2) DNS 滥用的当前定义和合同义务；以及 3) 竞争、消费者信任和消费者选择审核小组关于 DNS 滥用的发现和建议。我们希望通过此次讨论奠定基础，以便在蒙特利尔会议期间开展卓有成效、见地深刻的跨社群讨论。

为什么 DNS 滥用主题至关重要

全球网络犯罪损失逐年递增，据估计 2018 年已突破 6000 亿美元。[2] 网络罪犯纷纷利用乃至滥用 DNS 达成恶意企图，[3] 目前电子邮件仍然是最常用的攻击手段，[4] 针对消费者的网络钓鱼攻击急剧增长。[5]

若要使广大公众信任并依赖互联网开展通信和交易，DNS 基础设施管理当局必须采取措施，保障此类公共资源安全可靠。最新隐私法（包括欧盟《通用数据保护条例》）就公开域名所有人信息做出了限制，促使致力打击威胁的执法机构和网络安全专业人士陷入挑战，亟需恢复安全可靠的互联网环境。[6]

---

1 GAC 不但独立提出过这项建议，还通过公共安全工作组发表过建议。*参见范例*：GAC 公报：ICANN46 北京会议；ICANN53 布宜诺斯艾利斯会议；ICANN54 都柏林会议；ICANN57 海得拉巴会议；ICANN57、58 和 60 会议关于 DNS 滥用的 ICANN 社群演示；以及 2009 年执法机构建议（ICANN38 会议获得 GAC 通过）。

2 McAfee《网络犯罪对经济的影响 - 没有放缓》，网址为：https://www.csis.org/analysis/economic-impact-cybercrime Accenture《2019 年网络犯罪成本》，网址为：https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

3 *参见范例：*Symantec《互联网安全威胁报告》（2019 年 2 月），网址为：https://www.symantec.com/security-center/threat-report

4 Verizon《2019 年数据泄露调查报告》，网址为：https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations- report.pdf

5 Akamai《2019 年互联网现状》，网址为：https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial- services-attack-economy-report-2019.pdf

6 *参见范例：*反网络钓鱼工作组与信息传递、恶意软件和移动反滥用工作组联合开展的 ICANN GDPR 和 WHOIS 用户调研，网址为：lhttps://www.securityskeptic.com/2019/03/facts-figures-whois-policy-changes-impair-blacklisting-defenses.htm

章程要求 ICANN 在近期和持续审核中强调以下几个方面的重要意义：

- **处理 DNS 安全性和稳定性的挑战和威胁的安全工作的效果**，以及**安全工作可在多大程度上应对未来安全挑战**和威胁；[7]
- 新顶级域名授权数目增加之前或期间的**消费者保护**、安全、稳定与弹性、**恶意滥用**问题、主权关切和权利保护；[8]
- **改善通用顶级域名注册数据的准确度和访问权限**，并考虑保护该类数据的保护措施；[9]
- **当前 gTLD 注册目录服务**的**有效性**，以及**这项服务的推行是否能够满足执法工作的合理需求、促进消费者信任**和保护注册人数据[10] [着重部分由作者标明]

此外，ICANN 正在构思第二轮 gTLD 申请工作框架，为在合同激励措施中采用最佳实践创造了新的机遇，从而减少此类滥用及增加滥用用户或犯罪分子的犯罪成本。

因此，现在正是反思这些问题及考察最优路径的最佳时机，从而支持履行 ICANN 保持**并增强**对 DNS 管理的承诺，包括“DNS 和互联网的运营稳定性、可靠性、安全性、全球互用性、弹性和开放性。”[11] 在这一方面，政府和公共权威机构尤其具有发言权。[12]

DNS 滥用的当前定义和 ICANN 合同义务

竞争、消费者信任和消费者选择 (CCT) 审核小组由多个 ICANN 社群利益相关方组建而成，积极比较新 gTLD 与传统 gTLD 中 DNS 滥用的区别，细致考察 ICANN 社群现行的 DNS 滥用定义，进而评估现有保护措施是否充分。[13] 指出 ICANN 社群研究结果证明，“关于哪些情况构成 DNS 安全滥用或 DNS 基础设施的 DNS 安全滥用，存在着广泛的共识，”**CCT 审核小组将 DNS 滥用定义为“积极利用 DNS 和/或域名注册程序进行的蓄意欺骗、纵容或未经允许的活动。”**[14] CCT 报告使用术语“DNS 安全性滥用”指代更具有技术含量的恶意活动形式，例如恶意软件、网络钓鱼、僵尸网络，以及用作这些滥用形式的传递方法的垃圾邮件。[15]

上述定义与 ICANN 注册管理机构和注册服务机构的标准合同一致。根据 ICANN 标准注册管理机构协议的要求，新 gTLD 注册管理运行机构应在其注册管理机构-注册服务机构协议 (RRA) 中订立相关规定，禁止注册人实施以下行为：

---

7 ICANN 章程第4.6 (c) 节：安全、稳定与弹性审核。
8 ICANN 章程第 4.6 (d) 节：竞争、消费者信任和消费者选择审核。
9 ICANN 章程第 4.6 (e) 节：注册目录服务审核。
10 *同上*。
11 ICANN 章程第 1.2(a) 节：承诺。
12 切实认清政府和公共权威机构在处理引发公共政策问题的事件方面发挥的重要作用是 ICANN 的核心价值之一。ICANN 章程第 1.2(b) 节：核心价值。
13 *参阅*《CCT 最终报告》（2018 年 9 月 18 日），第 88-109 页。有关 ICANN 社群如何定义滥用的更多信息，请参阅《注册滥用政策工作组最终报告》（2010 年 5 月 29 日）：https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf
14 《CCT 最终报告》，第 88 页，以及附带资料。*另请参阅*《防止 DNS 滥用的新通用顶级域项目保护措施：修正报告》（2016 年），第 3 页。
15 《CCT 最终报告》，第 8 页。

> 散布恶意软件、滥用僵尸网络、网络钓鱼、盗版、商标或版权侵权、欺诈或欺骗行为、伪造或以其他方式参与违反适用法律的活动，并（依据适用法律和任何相关程序）注明这些行为或活动会带来的后果，包括中止域名。[16]

此外，注册管理运行机构必须“定期进行技术分析，以评估 TLD 中的域是否用于实施安全威胁，**如**网址嫁接、网络钓鱼、恶意软件和僵尸网络。”[17] [着重部分由作者标明]。我们发现，此列表仅供说明，并非完整列表。除了注册管理机构规定外，ICANN 注册服务机构标准合同要求注册服务机构及时“调查并适当地回应滥用举报。”[18] ICANN 多利益相关方社群发布的上述材料共同构成对 DNS 滥用的基本共识。

CCT 审核小组发现 DNS 滥用集中于特定的注册管理机构和注册服务机构并提出建议

CCT 小组注意到，域名通常是网络犯罪的关键部分，广泛用于协助恶意软件散布和僵尸网络命令与控制。同时发现，垃圾邮件营销活动通常与网络钓鱼和其他网络犯罪相关。[19] 值得注意的是，审核小组指出：

> 虽然 ICANN 注册管理机构和注册服务机构的标准合同规定一致使用指定的保护措施，但是各签约方为打击域名滥用所付出的努力存在很大差异。有些实体在收到投诉之前不会采取任何行动。与之相反，有些注册服务机构则会积极采取措施，例如，检查注册人凭证、阻止与已知网络钓鱼目标相似的域名字符串，以及仔细审查域名分销商。域名分销商并不是 ICANN 签约方，因此不直接受 ICANN 对标准合同要求的执法权约束。[20]

为进一步了解新 gTLD 保护措施的有效性，CCT 审核小组开展了一项研究，分析 2014 年到 2016 年期间全球 gTLD 中垃圾邮件、网络钓鱼和恶意软件散布的发生率，区分传统 gTLD 与新 gTLD，发布了后续报告。[21] 值得注意的是，DNS 滥用研究表明 DNS 中存在严重的滥用问题。关于新 gTLD 项目，研究指出在某些新 gTLD 中，注册域名滥用现象超过 50%。[22] 同时，研究还强调了另外一些重要发现：

- 越来越多的不法分子将新 gTLD 视为攻击目标。
- 传统 gTLD 中的被入侵域比例较高，同时不法分子往往还会选择使用某个新 gTLD 恶意注册域名；
- 滥用率最高的新 gTLD 的注册管理运行机构在价格上具有竞争力；
- 新 gTLD 中的网络钓鱼和恶意软件滥用率逐渐与传统 gTLD 趋同；
- 网络钓鱼攻击中使用的域名最集中在五个新 gTLD 中，这五个新 gTLD 占所有列入反网络钓鱼工作组黑名单的新 gTLD 域名的 58.7%；

---

16 《ICANN 注册管理机构协议》，规范 11 第 3(a) 条。

17 《ICANN 注册管理机构协议》，规范 11 第 3(b) 条。此条是一项重复主题，论述因 ICANN 实施这项保护措施引发的各类 GAC 问题、顾虑和建议，同时要求注册管理机构监控安全威胁，但注册管理运行机构无义务采取行动应对安全威胁。*参阅*《新加坡公报》（2014 年）、《洛杉矶公报》、《伦敦公报》。GAC《北京公报》不仅将监控安全威胁列为义务，还要求在检测到某些极端安全威胁时做出响应。GAC 建议，当发生造成“实际危害”的安全威胁时，注册管理运行机构将通知相关注册服务机构；如果注册服务机构未“立即采取行动”，则“暂停该域名，直到解决问题为止。《北京公报》，第 7 页。

18 ICANN《注册服务机构协议》第 3.18 条。

19 《CCT 审核小组最终报告》，第 93 页。

20 《CCT 审核小组最终报告》，第 93 页。

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

22 关于 gTLD 中 DNS 滥用的统计分析最终报告（2017 年 8 月 9 日）：https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

- 2016 年第四季度，新 gTLD 的垃圾邮件百分比明显高于传统 gTLD（比传统 gTLD 高出 10 倍）；
- 为达到恶意目的而注册的域名通常包含与商标术语相关的字符串。
- 滥用数量主要与严格注册要求有关：*即*，不法分子喜欢注册标准新 gTLD（通常可公开注册）域名，而不愿注册社群新 gTLD 域名（注册管理机构可能对注册域名的人员或实体做出限制）。

CCT 审核小组得出结论：诸如注册限制、价格和注册服务机构特定做法之类的因素似乎更有可能影响滥用率。[23] 因此，CCT 审核小组建议：

- ICANN 组织协商修订现有的《注册管理机构协议》；或者，考虑制定与新 gTLD 后续轮次关联的新《注册管理机构协议》，**在相关协议中纳入可提供激励措施的规定，包括为注册管理机构（特别是开放的注册管理机构）提供财务激励，进而促使他们采取积极主动的反滥用措施** [着重部分由作者标明]；
- ICANN 组织协商修改《注册服务机构认证协议》和《注册管理机构协议》，以纳入旨在防止系统地利用特定注册服务机构或注册管理机构进行技术性 DNS 安全性滥用的规定。特别是，ICANN 应建立滥用门槛，达到此类门槛时会自动触发合规性查询，注册服务机构和注册管理机构在达到更高的门槛时会被认定为违反其协议；
- 通过委托进行持续数据收集，包括但不限于 ICANN 域名滥用活动报告 (DAAR) 举措，进一步研究特定注册管理运行机构、注册服务机构与 DNS 安全性滥用之间的关系。为了确保透明度，应该定期公布此信息，最好是每季度一次或每年至少一次以便能够识别需要 ICANN 组织加强审查、调查和潜在强制措施的注册管理机构和注册服务机构。在确定滥用现象后，ICANN 应该制定行动计划，以回应此类研究、纠正已识别的问题，并确定未来的持续数据收集工作；以及
- ICANN 应该收集相关数据，并公布对 gTLD 域名注册负责的各方。

ccTLD 注册管理机构最佳实践

近年来，越来越多的 ccTLD 注册管理机构采取积极主动的反滥用措施缓解通过 DNS 开展的犯罪活动，尽量减弱域名对不法分子的吸引力，避免区域滥用及抵制不法分子。具体措施包括强化身份验证方法（涵盖身份核实）[24] 以及采用基于数据的欺诈预测模型，此类模型综合运用数据注册和基础设施衡量标准，识别并预测出于不良目的注册域名的行为。[25] gTLD 注册管理机构和注册服务机构应推行这些久经考验的最佳实践。

结论

本社群得天独厚，在评估和选择防范 DNS 滥用的公共政策方面发挥着重要作用。我们赞同注册管理机构利益相关方团体工作组的观点：为使产品（当然也包括 DNS）大获成功，必需提供值得用户信赖且信誉良好的产品。为更有效地解决 DNS 滥用问题及推广应用更值得信赖的 DNS，建议社群认真考虑采纳上述建议，因为其中提出了可以*（并且应当）*用于解决 DNS 滥用问题的可行性措施。GAC 期待在 ICANN 66 蒙特利尔会议期间与其他社群团体讨论这一主题。

---

[23] 《CCT 最终报告》，第 94 页，引用 DNS 滥用研究，第 24-25 页。

[24] 参见范例：ICANN64 会议经验：.DK 如何成功减少域名滥用、https://www.dk-hostmaster.dk/en/news/mandatory-identification-nemid 和 https://www.dk-hostmaster.dk/en/news/dk-hostmaster-makes-online-fraud-more-difficult

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