技术白皮书 · 框架提案 · 1.0版

从发现到 实施应对措施

一套可衡量的 DNS Abuse 应对架构：涵盖证据来源与保管链、相称行动、公共问责和快速申诉；其目的在于接受检验，而非仅供宣称。

发布于2026年8月2日 | PhishDestroy 研究 | 公众咨询草案 | 未经同行评审

PD-WP-2026-01 · 版本 1.0 · 发布于 2026 年 8 月 2 日
永久链接：https://phishdestroy.io/zh/dns-abuse-enforcement-framework

摘要

独立提案 · 非ICANN项目

直接结论。 gTLD的合同生态系统中，存在一个可量化的差距：即从域名被技术验证为恶意使用，到采取有效缓解措施之间存在时间差。 已发表的研究表明，许多网络钓鱼活动会持续数小时甚至数天，而合同合规程序的执行则可能需要多个工作日。文中披露的情景模型展示了延迟如何增加预期活动收益；60%–85%这一区间是该论文对通知后损害的核心可验证估计值，并非针对全球所有欺诈行为的既定统计数据。 100–150美元的工程估算涉及对定义好的区域、证书透明度（CT）及公共数据源数据集的收集和初筛处理，而非法律审查或执法的全部成本。 该论文提出了签名证据、可量化的响应目标、经验证案件的自动升级、相称的补救措施、公开问责以及快速上诉机制。但并未建议赋予举报人直接访问域名暂停控制权限的权限。

- **原始资料** 有官方文件或已发表的研究直接支持。
- **示意图** 一种可重复的计算，其输入参数是假设，而非市场平均值。
- **政策建议** 一项供征询意见、测试和修改的设计方案。

01 研究问题、研究范围及证明标准

这个问题比"是谁失败了？"更具体： **在经验证的证据与采取相应行动之间，哪些可观察到的延迟是可以避免的？哪种干预措施既能减轻受害者所受伤害，又不会造成不可接受的误报或附带损害？**

本报告的范围涵盖gTLD生态系统中的签约方：注册人、转售商、注册服务商、注册管理机构以及ICANN的合同合规职能部门。仅当托管服务提供商、内容分发网络（CDN）、浏览器、支付服务、广告平台、国家计算机应急响应中心（CERT）和刑事司法机构对证据链或响应链产生影响时，才会将其纳入其中。 国家代码顶级域名（ccTLD）具有不同的治理结构，不被视为受 ICANN 的 gTLD 合同约束。

核心论点的现状

- 本文将ICANN视为gTLD生态系统中一个私营治理和合同履约机构。ICANN并非政府监管机构或执法机构，但它负责对注册商进行认证、与注册管理机构签订合同并执行相关协议；这种有限的职权范围并不免除其机构问责义务。
- 60%–85%这一区间是本文危害模型中的核心定量估计值。它被呈现为基于明确假设和案例观察得出的可验证估计值——而非针对全球所有欺诈行为的既定统计数据。 发布一份能够将检测、通知、缓解和危害的时间戳相互对齐的事件级数据集，是下一步的实证工作。

- 100–150美元这一数字，是针对在定义好的可访问区域内，基于通用基础设施上的证书透明度（Certificate Transparency）和公共数据源，进行持续收集和初步筛选的可验证工程预算估算。它并不包含实现完全全球可见性、法律审查、申诉、高可用性或执法所需的成本。 因此，本文将其视为一个基准，可通过已发布的工作负载、源清单和成本日志进行复现——而非一个已经得到验证的通用价格。这种区分虽然缩小了该主张的范围，但并未抹去正在测试的成本不对称性。
- 该论文为期三周的对比研究关注的是合规响应延迟，而非普遍适用的域名下线服务水平协议（SLA）。ICANN的 合同合规常见问题解答 该文件指出，大多数投诉类型在正式上报前可经历三个连续的、各为五个工作日的响应期，而许多恶意活动则会持续数小时或数天。合同另行规定，在获得可采取行动的证据后，必须立即采取适当的缓解措施。 [2] [4]
- 对于经核实的、单一目的的恶意注册，`serverHold` 这是最具破坏性的DNS级补救措施之一，因为它会从该区域中移除委派。但该措施并非万能：它也可能干扰邮件、子域名和合法服务；缓存的响应可能会一直保留到TTL过期；此外，对于遭到入侵或共享的服务，可能需要采取更针对性的缓解措施。 [4] [7]

研究贡献

该提案是可证伪的。一项试点研究可以针对分诊时间、缓解时间、伤亡替代指标、复发率、假阳性率、逆转时间以及附带影响等指标，对干预组和对照组进行比较。

02 原始资料所证实的内容

$165.1M

ICANN FY27 运营资金

已通过FY27预算。按实际情况调整规模；并非DNS Abuse的支出。 [1]

191,561

2025年IC3收到的网络钓鱼/冒充投诉

按投诉数量计算，IC3投诉中占比最大的类别；直接归因的损失达2.158亿美元。 [10]

24 小时

2021年一项研究中的中位生存期

这是针对1,288个网络钓鱼域名的特定数据集结果；并非普遍的存活周期。 [11]

无固定服务水平协议（SLA）

统一下架截止日期

2024年的修订案采用了“及时”和“适当”的减缓措施，而非设定一个统一的截止日期。 [2] [3]

提案	状态	可以这样说
网络钓鱼属于 DNS Abuse	已验证	网络钓鱼明确属于 2024 年 gTLD 合同修订所涵盖的五类行为之一。 [2]
注册商必须采取行动	已验证	注册商在掌握可采取行动的证据，表明其管理的域名被用于 DNS Abuse 时，必须迅速采取行动。 [2]
注册局必须采取行动	已验证	注册局运营方在根据可采取行动的证据合理认定某注册域名被用于 DNS Abuse 时，必须迅速采取行动；具体措施仍取决于具体情境。 [3]
`serverHold` 撤销委托	已验证	这是由服务器设置的EPP状态。缓存的DNS响应可能会保留至过期，且该操作将影响整个已注册域名。 [7]
所有 DNS Abuse 均可通过 CZDS 或 CT 观察到	错误	CZDS 和 Certificate Transparency 是有价值的传感器，但不能完整、实时地反映所有域名使用情况。 [8] [9]

ICANN关于落实2024年修订案中合同要求的首次半年报告显示，共开展了192项调查，暂停了2,700多个域名，关闭了350多个网络钓鱼页面，并发布了两份违规通知。 这些数据虽不能证明现行管控措施已足够完善，但足以驳斥“该系统完全不采取任何行动”这一绝对性说法。 [5]

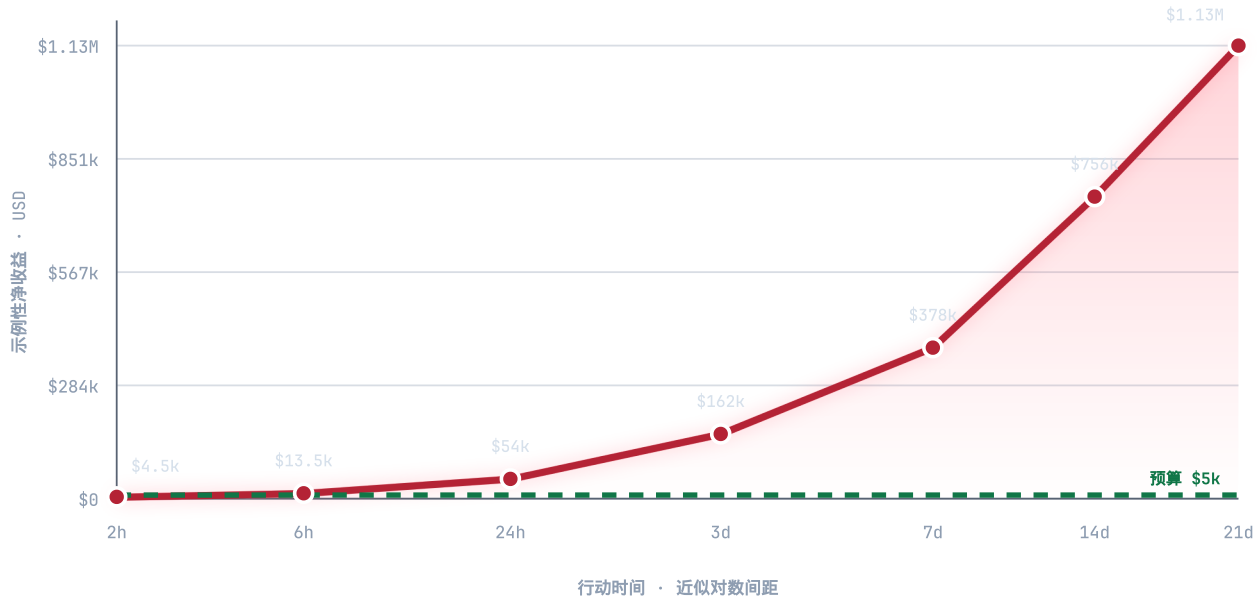
03 为什么响应延迟仍然是一个有价值的研究课题

某些网络钓鱼活动的时间跨度以小时或天为单位。Bijmans等人在一项2021年的研究中指出，对1,288个网络钓鱼域名的观察显示，其平均存活时间为45小时，中位数为24小时。 [11] 一项针对2026年新注册钓鱼域名的研究显示，其分布极不均衡：在14,112个可测得存活时间的域名中，平均存活时间为8.6天，中位数为1天。 [12] 虽然这两个样本都不能推广到所有威胁类别，但它们都说明了为什么仅以工作日为单位衡量的流程可能会遗漏短暂的欺诈和网络钓鱼活动。

> **测得的时间错配**
>
> 这些研究并未确定在收到通知后发生的财务损失所占的比例，但确实证实了时间上的错配：对于平均持续时间接近一天的攻击活动而言，一个早期非正式合规阶段就可能耗时长达十五个工作日的流程，本身无法作为事件响应措施。 因此，下文提到的“21天”仅是一种合规延迟的情景，而非适用于所有情况的“ICANN服务水平协议（SLA）”的标签。

图1 · 欺诈和网络钓鱼行动的累计结果示意图

模型 · 对数型时间间隔



该曲线直观展示了第4节中的情景；它并非观测到的市场数据。为便于阅读，水平方向上对较长的区间进行了压缩。来源：可复现模型，输入参数已公开。

因果谨慎

域名存活时间缩短并不一定意味着能避免经济损失。攻击者可能会转移阵地、利用已被入侵的网站、更改传播渠道，或在被发现前套现。必须对因果关系进行量化评估，而不能仅凭下线速度来推断。

04 作为可复现情景的欺诈和网络钓鱼活动经济分析

从经济角度来看，真正有价值的往往不是注册费，而是围绕一个域名积累的流量、创意、基础设施和信任。这种直觉是合理的；其具体规模因欺诈和网络钓鱼活动的不同而有所差异。因此，下方的计算器会显示所有输入数据，而不是将假设结果作为观察到的平均值呈现出来。

模型定义

```
visits(T)   = daily_traffic × T / 24
victims(T)  = visits(T) × conversion_rate
proceeds(T) = victims(T) × average_loss × (1 - cashout_attrition)
profit(T)   = proceeds(T) - campaign_budget
```

场景计算器

更改任何假设。这些数值仅供说明，并非对典型网络钓鱼市场的估算。

示例模型

欺诈和网络钓鱼活动预算（USD）

5000

每日访问量

2000

受害者转化率（%）

1.5

每位受害者的平均损失（USD）

2400

提现流失率（%）

25

行动时间（小时）

24

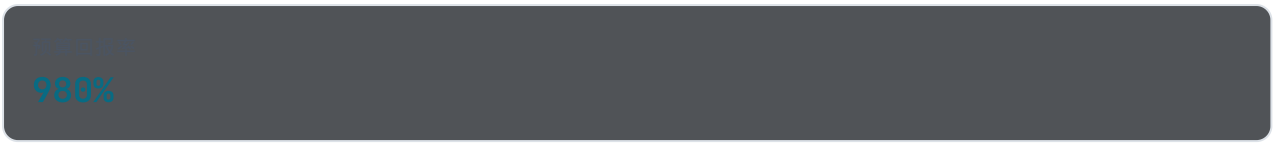
2,000

30

$54,000

$49,000

2.2 h



该模型表达的是期望值，因此预计受害者人数可能出现小数。模型未考虑流量衰减、检测后的行为变化、活动向其他基础设施转移、受害者重复计算以及不确定性分布。

▶ 查看模型源表

05 在不追求过分精确的情况下衡量可预防的伤害

只有在对“检测”、“交付”和“危害”进行一致定义的情况下，“检测后的损失”才能成为有意义的评估结果。黑名单上的时间戳并不能证明注册商已收到可采取行动的证据。钱包交易并不自动归因于某个特定域名。域名无法访问并不意味着能够确定是哪一方导致了这一变化。

最小事件模式

活动	所需的时间戳	最低证明
第一项观察结果	t_obs	传感器、请求/响应哈希、捕获方法、时钟源。
技术验证	t_valid	可重复性指标、评审人身份、威胁类别和置信度。
已送达通知	t_notice	经认证的送达回执及证据汇编版本。
责任方承认	t_ack	案件编号及目标角色：主机、注册商、注册局、平台或主管机构。
观察到缓解情况	t_mitigate	DNS、HTTP、支付或平台状态，从多个角度进行监测。
申诉 / 恢复	t_restore	决策依据、证据变更及恢复验证。
伤害事件	t_harm	经过去识别化的受害者报告、可追溯的交易记录或其他有据可查的替代证据。

拟议的成果指标

```
Post-notice harm share =
  attributable harm with t_harm > t_notice
  ----------------------------------------
  all attributable harm in the observation window
```

分子和分母必须采用相同的归因规则。 结果应报告队列、置信区间、右截尾、数据缺失来源、重复受害者处理以及对观察窗口的敏感性。术语“可预防”应仅用于因果设计，或至少用于配对比较——而非通知后发生的每一事件。

中心模型估计值 · 60–85%

该论文将60%–85%作为其核心估计值，用于表示在所建模的事件类别中，在检测和通知之后发生的归因损害所占的比例。 这是基于已披露的假设和案例观察得出的情景估计值——而非针对全球所有欺诈行为的实测统计数据。在尚未获得能够将观察结果、经验证的证据、事件发生、缓解措施及损害时间戳相互匹配的事件级数据集之前，该估计值应用于敏感性分析。发布该数据集才是对该论点的证据检验，而非删除该论点的理由。

06 制度图谱：能力是分散的

没有任何单一参与者能够全面掌握或控制整个事件。注册商了解注册人与域名之间的关系；注册局控制注册局所管辖域名的状态；主机和CDN控制内容分发；浏览器和安全厂商控制警告提示；支付和钱包服务商可以中断转账；相关机构可以强制要求保留或扣押数据。ICANN在gTLD生态系统中制定并执行合同，但并不运营一个通用的EPP控制平面。

01 · 信号

研究人员与传感器

观察内容、基础设施和受害者指标；保留证据来源与保管链。

02 · 服务

主持人 / CDN / 平台

可以快速删除内容或访问权限，通常无需更改域名。

03 · 受托方

注册商

审查 DNS Abuse 报告，联系注册人，并可设置客户端 EPP 状态。

↓

04 · ZONE

注册局运营方

控制注册表中EPP的状态以及TLD区域的委派。

05 · 合同

ICANN 合规

负责调查合同方的合规情况；并不对每起欺诈案件作出裁决。

06 · 法律

CERT / 主管部门

协调应对措施，并行使各管辖区域特有的法律权力。

权限的分散并不意味着责任的消解。赞助注册商将滥用处理工作委托给经销商，并不意味着其合同义务就此免除；注册局负责控制服务器设置的EPP状态；ICANN负责监督合同合规性。 审计追踪记录不仅必须记录采取行动者，还必须记录谁接收了可采取行动的证据、谁将案件转交、谁未予回应或谁未履行分配的职责。法律授权仍归属于有权采取措施的行动者；问责制同样涵盖有据可查的失职行为。

资金集中与一项可检验的激励冲突假说

$165.1M

2027财年"ICANN"运营资金

通过了2027财年的基准预算案。[1]

≈98.1%

注册库和注册商费用来源

在1.651亿美元的融资计划中，约有1.62亿美元。[1]

70.7%

仅交易费

$116.8M tied to billable domain transactions.[1]

因此，该资金结构高度依赖于合同方支付的款项——ICANN负责执行这些合同——且其中很大一部分随可计费的注册交易量而波动。这形成了结构性依赖，并引发了一个关于激励冲突的合理质疑。它确实 不.....仅凭这一点，尚不足以证明存在蓄意执法不力或已形成的"监管俘获"。应结合个案层面的响应时间、执法结果、处罚措施、违规再犯情况，以及获得资助的利益相关方在政策制定和实施决策中的作用，对"监管俘获"假说进行检验。

07 2024年合同基准——以及其中未明确规定的内容

2024 年 4 月对《注册商认证协议》和《基础注册局协议》的全球性修订，明确规定了缓解 DNS Abuse 的义务。注册商在掌握可采取行动的证据，表明其管理的域名被用于 DNS Abuse 时，必须迅速采取行动。注册局运营方在根据可采取行动的证据合理认定某注册域名被用于 DNS Abuse 时，必须迅速采取行动。在这两种情况下，适当措施取决于具体情境、严重程度和附带损害。[2][3]

三个常被混为一谈的时间线

时间轴	适用范围	这并不意味着什么
24小时	根据 RAA §3.18.3，审查由执法机构、消费者保护机构、准政府机构或类似机构向专用联系人提交的、有充分依据的非法活动报告。	这并非一项适用于所有情况的24小时暂停期限。
"及时"	在达到适用的可采取行动的证据门槛后，采取适当的缓解措施。	这并非固定的小时数，且并非每个案例都需要采取相同的补救措施。
21天	可在正式的合同违约通知发出后作为补救期出现。	这并非每个被报告的恶意域名所拥有的普通有效期。

这种灵活性有其优势：遭到入侵的大学域名不应像新注册的单一用途钓鱼域名那样处理。问责方面的问题在于，如果没有公开的时间戳、案件类别和结果代码，就很难对"及时"和"适当"进行比较。下文提出的建议增加了评估和审查机制，同时并不假装一个截止期限能适用于所有情况。

08 界限问题：网络钓鱼已涵盖在内；但某些金融欺诈行为可能未被涵盖

网络钓鱼明确属于 DNS Abuse 的合同定义。更难界定的是以自有名称欺骗用户、而非冒充可识别第三方的网站，例如部分虚假投资平台、欺诈商店、追款骗局和钱包签名骗局。视具体事实而定，这些行为可能被归类为网站内容层面的违法行为、消费者欺诈或其他法律类别，而不是合同意义上的 DNS Abuse。

> **拟议的研究标签**
>
> **经核实的金融损害型滥用（VFHA）**：指有文件记录的域名使用行为，其目的在于通过欺骗获取资金、支付凭证、私钥或助记词，无论是否冒充品牌。VFHA 不是 ICANN 的现行术语，本身也不会产生合同授权。

政策咨询可研究，像 VFHA 这样范围狭窄、以证据为基础的类别，应纳入未来合同、跨行业转介框架还是国家法律。扩大范围必须要求精确的损害检验、可靠证据、相称救济、管辖权审查和申诉。含糊的“诈骗”标签并不充分。

09 每月100–150美元的监控费用主张必须证明什么——以及它无法证明什么

一台通用服务器可以下载参与“证书透明度”（gTLD）计划的区域文件的可用快照并在本地计算变更，接收选定的证书透明度事件和公开数据源，对字符串进行规范化处理，计算哈希值并确定候选项的优先级。这是一个实用且可测试的工程基准——而非“对互联网的全面监控”。 2026年第二季度，威瑞信（Verisign）报告称所有顶级域名（TLD）的注册量共计4.016亿个；CZDS覆盖的是参与的“安全域名”（gTLD）区域文件，而非所有顶级域名；而CT则记录的是公开日志中的证书或预证书，而非每个活跃或有害的域名。 [8] [9] [17]

能力	通用原型	生产级公共利益服务
区域/CT/数据源接入	适用于确定的来源集合	冗余收集器、来源合同、缺口监控
字符串/哈希分流	可行	基准测试、漂移检测、假阴性研究
浏览器渲染	小规模抽样子集	隔离执行集群、区域观测点、恶意软件遏制
法律认定	不包括	合格审核人员、管辖权和权限映射
高可用性 / 证据保留	通常不具备	HSM 支持的签名、审计日志、备份和事件响应
申诉与恢复	不包括	24/7 运行、独立升级和服务目标

图2 · 数量级背景 对数宽度 · 非同类成本

样本采集与初筛层 · 年度 $1.2k–$1.8k

韧性基础设施情景 · 年度 $10.4k

全员参与的项目方案 · 年度 $500.4k

ICANN 2027财年运营资金 · 年度 $165.1M

采用对数宽度可确保较小数值清晰可见。 前三个数字是已公开的工程或项目假设，需要以已发布的基准数据为依据，并非供应商报价。ICANN 运营资金是一个经过验证的机构级数据。这些预算数字是刻意设为不等值的：此比较旨在检验基础数据收集和分拣是否本身就是一项难以承受的成本，而非检验完整的执法项目是否每月需花费100美元。

10 拟议的经核实 DNS Abuse 响应框架

该框架是一个参考架构，而非自动的全球紧急关闭开关。它对案件范围、决策记录和时间戳进行了标准化，同时允许授权操作员选择干扰最小且有效的措施。

01 · 数据导入

获取与保存

收集报告和观测数据；对原始数据进行哈希处理；同步时钟。

02 · 证据来源与保管链

证据标准化

记录来源、方法、处理历史和来源依赖关系。

03 · 验证

证实

重现有害行为，并区分独立证据。

↓

04 · 评估

风险与担保

对恶意注册、遭入侵的服务、共享主机及其严重程度进行分类。

05 · 回复

通报与缓解

指定责任方、目标时间以及对运营干扰最小且有效的补救措施。

06 · 回顾

审计与申诉

发布结果元数据，衡量影响，并支持快速纠正。

证据等级

E1 **未经验证的信号**

单条信息、词汇匹配或声誉指控。适合作为观察依据，但仅凭此绝不足以作为暂停账号的依据。

E2 **可重现的行为**

带有时间戳的捕获记录，显示了凭证盗取、恶意软件传播或欺骗性交易路径。

E3 **独立核实**

至少两个真正独立的来源，或者一个可复现的技术证明，外加所有权/背景核查。

E4 **符合条件的确认**

权威机构、受影响的服务、品牌所有者或经核实的受害者证据，并具备符合隐私保护要求的证据链。

独立法则

复制同一上游阻止列表的三个源应视为一个来源，而不是三个。证据来源与保管链图必须显示共同起源、同步关系和供应商再发布情况。

11 最小证据包与可互操作的 API

API应创建一个可验证的案例，并启动一个可审计的响应计时器；报告人不得直接发出暂停命令。如果某个E3/E4案例涉及单一目的的恶意注册，且在未作出合理裁决或采取有效缓解措施的情况下到期，系统将自动将其上报给注册管理机构或具有合同或法律授权的其他主体。A `serverHold` 该命令只能由授权主体发出。自动权限提升以及在授权到期时采取行动的注册权限，是拟议的政策变更，而非对现有权限的声明。每次状态转换都会被签名并附于审计日志中。

POST /V1/CASES · 示例

```
{
  "indicator": {"type": "domain", "value": "example.invalid"},
  "alleged_category": "credential_phishing",
  "observed_at": "2026-08-02T06:14:22Z",
  "evidence": [
    {
      "type": "http_capture",
      "sha256": "a3f1c9…",
      "collection_method": "isolated_browser_v2",
      "source_id": "reporter:ed25519:7c2a…"
    }
  ],
  "provenance_graph": "ipfs-or-object-store:sha256:91bd…",
  "collateral_context": {
    "registered_domain_scope": true,
    "shared_service": false,
    "mail_observed": true,
    "suspected_compromise": false
  },
  "requested_action": "review",
  "reporter_signature": "ed25519:…"
}
```

成功的响应将返回案件编号、受理方、证据等级、完整性错误、目标审查时间以及公开透明度链接。在主管机构评估权限及连带影响之前，不得承诺采取任何具体补救措施。

12 建议设定响应目标，而非统一的下架期限

服务级别目标应区分开来 *致谢*, *分诊*, *决定* 和 *有效的缓解措施*. 这使得性能可以被量化评估，同时并不预设停权总是正确的处理结果。

案例简介	致谢	分诊目标	决策目标	典型回答选项
在单一用途的恶意注册中窃取 E3/E4 支付凭证或助记词	15分钟	1 小时	4 小时	内容块；经授权的注册商/注册局暂停服务；浏览器和支付警告。
E3 品牌钓鱼或恶意软件传播	30分钟	2 小时	6 小时	根据控制点，执行主机/CDN清除、域名缓解、黑洞处理或发出警告。
遭到入侵的合法域名或共享的 SaaS 租户	1 小时	4 小时	12 小时	路径/账户隔离及所有者恢复；尽可能避免暂停已注册域名。
存在分类争议的财务欺诈	4 小时	12 小时	24 小时	保留、平台/支付干预、主管部门转介及合理决定。
E1信号或报告不完整	自动	24 小时	在验证完成前无数据	进行监控、补充材料并要求提供证据。

这些是试点目标。正确的数值应根据观测到的威胁持续时间、人员配置、错误成本和法律限制来推导，并以达成率分布的形式公布，而非仅给出单一平均值。

13 安全性、正当程序、隐私和故障模式

如果没有相应的防护措施，过快的响应可能会将错误数据放大，进而导致审查、商业破坏或基础设施中断。因此，一个合理的架构应将误报和附带损害视为首要的安全故障。

失效模式	必需的控制	可审计指标
针对竞争对手的恶意举报	报告方身份认证、来源信誉度、独立复现以及针对恶意举报的制裁措施	按报告方划分的报告驳回率；经确认的操纵案例
打着“共识”幌子的信息循环	证据来源图与上游来源去重	谱系校正前后独立来源计数
被入侵的合法域名被批量暂停	注册意图分类与路径级缓解偏好	受感染域名的共享；受影响的合法服务
受害者数据或漏洞利用细节被公开泄露	分级披露、信息遮蔽、证据封存及保存期限	隐私事件；信息遮蔽审查结果
不当行为仍在持续	全天候（24/7）申诉受理服务、独立审核人员及经过认证的修复流程	中位数和第95百分位数的逆转时间
注册局暂停服务导致电子邮件/子域名服务中断	担保品清单、救济措施的相称性及诉讼后监督	每次操作导致的服务中断情况；回滚率

正当程序的最低保障

1. 每项限制性措施都会记录其原因代码、证据等级和负责决策人。
2. 登记人可以获取一份符合隐私保护要求的理由说明，并提交反证。
3. 紧急申诉将由未参与最初决策的人员进行复核。
4. 撤销操作通过与原始操作相同的有符号通道传播。

5. 汇总错误和恢复统计数据是公开的；敏感证据仍受访问控制。

14 从“毒性评分”到可追责的响应质量指数

公共注册商评分虽可提高问责制，但若仅凭简单的排名，其结果会因域名组合规模、数据源覆盖范围、客户构成以及域名是否被恶意注册或随后遭到入侵等因素而产生偏差。绝不能以评分作为理由，对某家注册商的所有客户实施集体封禁。

建议的质量向量

```
RQI = report as a vector, not a single opaque rank:

  coverage-adjusted validated-abuse rate
  median / p90 acknowledge, triage and decision times
  mitigation effectiveness and recurrence
  false-positive and reversal rates
  median / p95 appeal-resolution time
  evidence completeness and transparency rate

Always publish N, observation window, confidence intervals,
feed coverage and malicious-registration / compromise split.
```

如果治理工作需要使用综合评分，应在评估前设定权重，并针对保留样本进行敏感性测试和回测。结果应按TLD、注册商规模、威胁等级和证据来源进行分层。输出结果应为问责信号——而非自动生成的域名判定结果。

15 分级访问的公共 DNS Abuse 透明度数据库

透明度登记册可以消除关于通知是否存在、何时送达以及随后采取了何种行动等争议。然而，公开所有相关信息可能会泄露受害者身份、个人数据、调查方法以及正在使用的漏洞利用路径。解决之道在于分级访问权限。

P

公开记录

案件编号、指标、大类、关键时间戳、证据等级、行为主体角色、结果代码、申诉状态以及已封存证据的哈希值。

C

合同方视图

可复现的技术证据、联系渠道、相关背景及保存说明。

R

受限权限视图

受害者数据、资金溯源信息、正在调查的案件材料以及未经删节的证据链。

每次更新均为仅追加模式，并附有时间戳和数字签名。更正操作不会抹去历史记录，而是添加一条替代记录。公开搜索应遵守数据保留规则，防止大规模发现受害者信息，并为不准确的个人数据提供补救措施。

16 一项为期六个月的试点项目，附带预注册评估

一项有价值的试点研究应规模适中：既要便于管理，又要足以验证因果链。建议范围如下：三名志愿者注册机构、两名注册库运营商、一名托管/CDN合作伙伴、两个独立研究数据源以及一个符合资格的申诉专家小组。在分配病例之前，应先注册研究方案和结局定义。

第1个月

协议与法律映射

定义类别、授权机构、证据等级、隐私影响评估和终止条件。

第2个月

对现有流程进行工具化改造

在不改变响应行为的情况下，测量基线时间戳和结果。

第3个月

运行证据包

引入签名的证据来源、去重和附带影响分类。

第4个月

测试响应目标

对符合条件的病例进行随机分组，或采用阶梯式推广策略；每日监测错误情况。

第5个月

申诉 练习及其失败情况

开展恢复演练、红队恶意报告演练以及访问控制审计。

第6个月

独立评估

应公布效应量、置信区间、缺失数据、不良事件、成本及重复实验材料。

试点的主要结果

- 从经验证的证据到有效缓解措施所需时间的中位数和第90百分位数。
- 通知后可归因损害的差异，或预先指定的受害者暴露替代指标。
- 假阳性率、错误操作的严重程度及恢复时间的中位数。
- 同一注册人、基础设施集群及欺诈/网络钓鱼活动层面的复发。
- 每例经确认病例及每项有效防控措施的直接运营成本。

> **决策规则**
>
> 仅在试点项目显示出显著更快的实际缓解效果，且未超过预先设定的误报、隐私事件、申诉延迟或附带服务中断限值的情况下，才进行规模化推广。

17 结论与可验证的建议

DNS Abuse 应对措施既不是纯粹的技术性筛选机制，也不是单一机构能够独自解决的问题。现有的2024年合同确立了实质性的减缓义务，但在证据、时机和补救措施方面留有相当大的裁量权。这种裁量权对于确保措施的相称性是必要的；但由于缺乏可比的记录，这也使得绩效评估变得困难。

1. **标准化证据包。** 在报告方、注册商、注册局和基础设施提供商之间采用通用的证据来源、时间戳和结果字段。
2. **分别测量各阶段。** 按威胁类别和证据等级，公布确认、分级、决策、缓解措施以及申诉的时间。
3. **区分恶意注册与系统遭入侵。** 对于遭到入侵的合法服务，应优先采取路径/账户修复措施，并将全域范围的措施保留用于那些采取此类措施才符合比例原则的情况。
4. **试点响应目标。** 针对高可信度、单一目的的恶意注册，应设定以小时为单位的目标，而非设定一个通用的截止期限。
5. **发布符合隐私保护要求的问责数据。** 使用分级透明度登记制度，其中包含已签署的历史记录和受限证据。
6. **评估因果影响。** 在预注册研究衡量受害者影响以及威胁向其他渠道或基础设施转移之前，不应将更快的暂停措施等同于减少了金钱损失。

这一建设性的结论并非在于，一旦对原问题的论点加以限定，该问题便不复存在。而是指核心论点现在可以接受检验了：检测后造成的危害范围在60%至85%之间，这是一个明确的定量假设； 100–150 是一个针对明确定义的传感器与分诊层的可验证工程预算假设；对于可信度高且目的单一的恶意注册，可以试点实施以小时为单位的响应目标。 公布工作量、成本、时间戳和结果，将其与基准进行比较，并衡量偏移量和误差。若得到证实，则可据此调整合同和政策；若被驳回，则可确定是哪项假设失效。

编辑声明与方法披露。 PhishDestroy 是一个独立的、非商业性的威胁情报项目。本文是一份政策与工程提案，并非法律建议、ICANN项目或经同行评审的论文。标注为“模型”的预算范围仅为规划假设。原始来源的论点链接如下。如有更正，

可通过本网站的联系渠道和负责任披露渠道提交。

第一人称立场 · 问责制必须既要遏制不作为，也要防止越权

执法权方面的个人界限

我并没有要求——也不想要——直接访问域名屏蔽工具。 该权限需要独立审查、公开的审计日志、快速的申诉机制以及可撤销性。

我相信有许多能力出众且负责任的公司，可以委托它们承担这项工作的部分内容。根据我的经验以及我发表过的文章，我不认为NameSilo属于这一类公司。

我不建议合法的美国公司将敏感的滥用行为处理或安全职能委托给那些在利益冲突、专业能力或行为表现方面经不起独立审查的特定承包商。这关乎有据可查的行为，而非国籍：仅凭俄罗斯背景本身并不能证明什么，正如仅凭美国公司的注册地址也无法证明什么一样。

我要求正义和切实的问责 对于那些通过注册和续费域名而获利，且这些域名已被证实与反复发生的诈骗活动有关的域名注册商。如果证据表明其行为已超出疏忽的范畴，而可能涉及明知故犯的协助——无论是直接参与运营，还是作为知情中间人，在多次警告后仍维持有害域名的注册和在线状态——此类行为应接受独立调查，若经证实属实，则应承担相应后果。 我并非将怀疑当作既定事实；但中介身份绝不能成为免于审查的借口。

审查相关调查 ↗

A

参考文献和来源注释

[1] **ICANN, Adopted FY27 Budget (2026)** · https://www.icann.org/en/system/files/files/adopted-icann-budget-fy2027-published-2026-en.pdf
1.651 亿美元 FY27 运营资金及其资金来源构成的依据。

[2] **ICANN, 2024 Global Amendment to the Registrar Accreditation Agreement** · https://www.icann.org/en/system/files/files/registrar-accreditation-agreement-global-amendment-05apr24-en.pdf
注册商 DNS Abuse 义务的主要合同依据。

[3] **ICANN, 2024 Global Amendment to the Base gTLD Registry Agreement** · https://itp.cdn.icann.org/en/files/registry-agreements/base-registry-agreement-global-amendment-05-04-2024-en.html
注册局运营方缓解义务的主要合同依据。

[4] **ICANN Contractual Compliance, DNS Abuse Obligations Advisory (2024)** · https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en
操作解释、报告要求和适当缓解措施示例。

[5] **ICANN, Enforcement of DNS Abuse Mitigation Requirements (2024)** · https://www.icann.org/en/system/files/files/icann-enforcement-of-dns-abuse-mitigation-requirements-08nov24-en.pdf
六个月实施报告，包括调查和缓解数量。

[6] **ICANN SSAC, SAC115: Report on an Interoperable Approach to Addressing Abuse Handling (2021)** · https://www.icann.org/en/system/files/files/sac-115-en.pdf
DNS Abuse 报告互操作性和证据质量的背景资料。

[7] **Hollenbeck, RFC 5731: EPP Domain Name Mapping (2009)** · https://www.rfc-editor.org/rfc/rfc5731.html
EPP 域名状态值的技术定义，包括服务器设置的状态。

[8] **Laurie et al., RFC 9162: Certificate Transparency Version 2.0 (2021)** · https://www.rfc-editor.org/rfc/rfc9162.html
关于CT作为传感器的权威协议规范及限制。

[9] **ICANN, Centralized Zone Data Service** · https://www.icann.org/en/contracted-parties/registry-operators/services/centralized-zone-data-service
参与的gTLD区域文件的范围和访问模型。

[10] **FBI Internet Crime Complaint Center, 2025 IC3 Annual Report** · https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
投诉和报案损失数据，包括网络钓鱼/冒充案件数量。

[11] **Bijmans et al., Catching Phishers By Their Bait (USENIX Security, 2021)** · https://www.usenix.org/system/files/sec21-bijmans.pdf
针对特定数据集对网络钓鱼基础设施及其观察到的存活时间进行的测量。

[12] **Newly Registered Domains and Phishing Lifetimes, Journal of Cybersecurity (2026)** · https://doi.org/10.1093/cybsec/tyag020
关于新注册的网络钓鱼域名及其生命周期分布的最新实证证据。

[13] **Inferential Analysis of Maliciously Registered Domains — INFERMAL (2024)** · https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf
ICANN -关于恶意域名注册及生态系统因素的资助性分析；对因果关系主张的相关限制。

[14] **Chainalysis, 2026 Crypto Scam Trends** · https://www.chainalysis.com/blog/crypto-scams-2026/
供应商对2025年链上诈骗资金流入量的预估；不计入域名钓鱼诈骗总额。

[15] **APWG, Phishing Activity Trends Report, Q1 2026** · https://docs.apwg.org/reports/apwg_trends_report_q1_2026.pdf
已观察到的网络钓鱼攻击/URL；该指标不等同于已注册的独立域名数量。

[16] **Cybercrime Information Center / Interisle, Phishing Landscape 2025** · https://www.cybercrimeinfocenter.org/phishing-activity-numbers-may-april-2025
将观察到的攻击、唯一域名和恶意注册的域名区分开来。

[17] **Verisign, Domain Name Industry Brief, Q2 2026** · https://blog.verisign.com/domain-names/q2-2026-domain-name-industry-brief-quarterly-report/
关于所有顶级域名（TLD）共计4.016亿个注册量的数据来源。