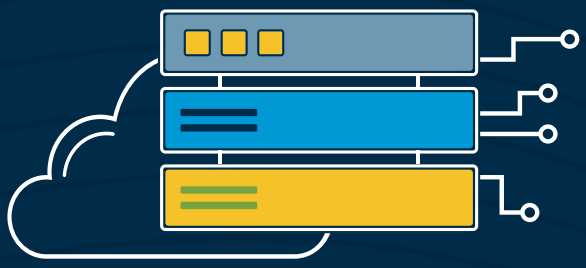
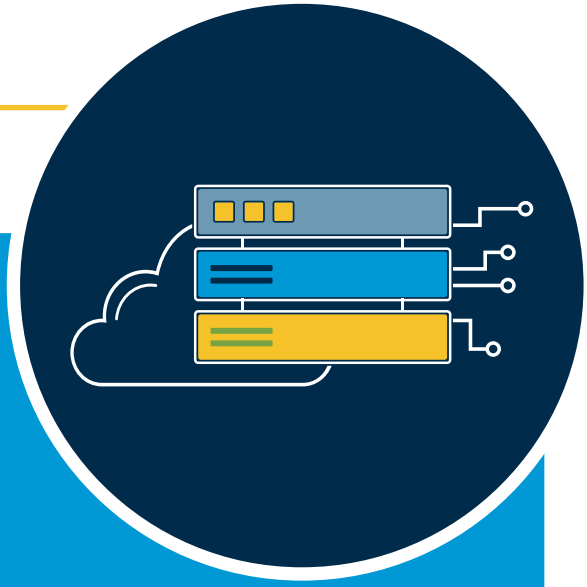


域名安全威胁信息搜集和报告 (DNSTICR)

2022 年 1 月

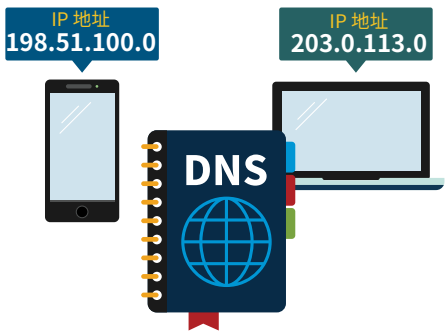
互联网名称与数字地址分配机构

ICANN



指南目录

什么是域名系统?



域名系统 (Domain Name System, DNS) 帮助用户在互联网上不会迷失方向。互联网上的每个设备或网站都有一个唯一地址——这类似于一个电话号码。该地址是一串复杂的号码，或一串号码和字母的组合，称为 **IP 地址**。IP 是互联网协议 (Internet Protocol) 的缩写。

IP 地址可能很难记忆。
DNS 则使互联网的导航更加容易。

IP 地址可能很难记忆。DNS 允许用户键入熟悉的字母——即：**域名**——而非 **IP 地址**，即可在互联网上徜徉。例如：您只需键入 **https://icann.org** 就可抵达 ICANN 的网站，而不是键入其 **IP 地址：192.0.43.7**。

什么是 DNS 安全威胁?

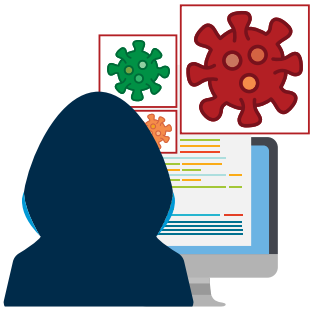
互联网领域中有各种形式的与内容有关的**滥用**行为。其中一些滥用行为包括为非法活动提供平台的网站，例如：剥削儿童和贩卖人口。还有一些网站则提倡网络霸凌，或成为销售本不存在或伪造产品的数字庇护港湾。

但 ICANN 的职权范围并不包括对互联网内容进行监管。

ICANN 将工作重点放在具体的 **DNS 安全威胁**之上，这类威胁的范围比涉及内容的滥用行为要更小。那么，什么是 DNS 安全威胁呢?

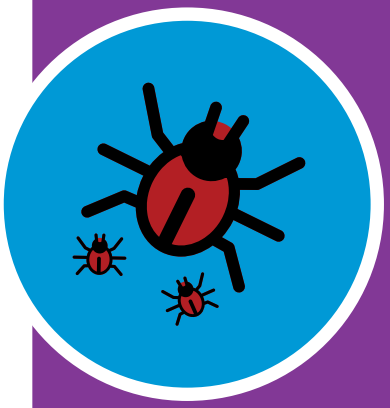
DNS 安全威胁包括任何旨在破坏 DNS 基础设施或导致 DNS 以非预期方式运行的恶意活动。

域名安全威胁信息搜集和报告 (DNSTICR)



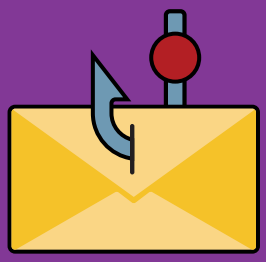
域名安全威胁信息搜集和报告 (Domain Name Security Threat Information Collection and Reporting, DNSTICR) 项目对 ICANN 组织认为利用 2019 冠状病毒病 (COVID-19) 疫情进行网络钓鱼或恶意软件活动的近期域名注册情况编制报告。

这些报告囊括了 ICANN 认为这些域名正在被恶意使用的证据。
这些报告与其他背景信息结合起来，可帮助负责任的注册服务机构确定正确的行动方案。



DNSTICR 是专门设计以搜索恶意软件注入和网络钓鱼企图的项目。

恶意软件
未经用户同意安装在一台设备上的软件，它破坏了这台设备的运行、收集敏感信息，或获得对私人计算机系统的访问权限。恶意软件包括：病毒、间谍软件、勒索软件和其他不需要的软件。



网络钓鱼
当攻击者通过发送欺诈性或外观相似的电子邮件或引诱用户使用仿冒网站，来欺骗受害者，使其泄露敏感的个人、企业或财务信息（例如：账号、登录凭证、密码等等），就发生了网络钓鱼。

DNSTICR 项目并无意于搜索以下与互联网有关的恶意行为：

僵尸网络

一组连接了互联网的计算机集合遭到恶意软件的感染，并被命令在一名远程管理员的控制下执行活动。

网址嫁接

通常通过 DNS 劫持或投毒，将用户重定向到欺诈性网站或服务。

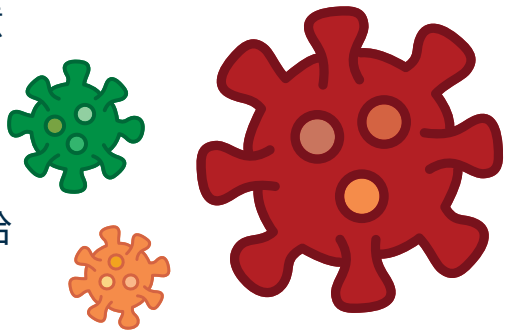
- 当攻击者使用恶意软件将受害者重定向到攻击者的网站，而不是最初请求的网站时，就发生了 DNS 劫持。
- DNS 投毒会导致 DNS 服务器或解析器以带有恶意代码的虚假 IP 地址进行响应。网络钓鱼与网址嫁接不同，后者涉及修改 DNS 条目，而前者则是欺骗用户输入个人信息。

垃圾邮件 （因为它被用来传播其他 DNS 安全威胁）

未经请求的批量电子邮件，收件人并未许可发送该邮件，且该邮件是作为一个更大邮件集合的一部分进行发送的，所有的邮件内容基本相同。一般的未经请求的电子邮件本身并不构成 DNS 安全威胁，但如果该电子邮件是网络钓鱼计划的一部分，则会构成威胁。

DNSTICR 项目的来源。

在 COVID-19 疫情期间，犯罪分子针对弱势群体、注意力不集中的人员、老年人、儿童和穷苦人员进行网络钓鱼。这些犯罪分子以世界各地的受害者为目标，使用多种语言来窃取金钱和个人信息。



犯罪分子和诈骗者通过致电、发送电子邮件或发短信给受害者，诱使他们透露个人信息，或购买伪造的疫苗接种凭证、伪造的 COVID-19 检测、或假冒治疗方案。

为了打击涉及 COVID-19 的互联网网络钓鱼和恶意软件，ICANN 组织开发了 **DNSTICR** 项目。该项目负责搜索并向注册服务机构报告域名的潜在恶意活动及其背景信息。此举在 ICANN 组织保护互联网用户免受 DNS 安全威胁的斗争中提供了另一层防御。

随着疫情持续肆虐，通过 DNSTICR 项目搜索到的专有名词和主题也会得到更新。这种更新是一个相对简单的技术流程。例如，额外的主题包括**护照 (passport)**，这与一些国家使用的**免疫证明护照 (immunity passports)** 有关；以及**伊维菌素 (ivermectin)**，这是一种与疫情有联系的抗寄生虫药物。

其他专有名词则可包括旨在为有需要的人员提供援助的、政府赞助的涉及 COVID-19 的著名项目的名称。更多的通用专有名词，例如：呼吸器、N95 口罩和消毒剂等，也被纳入其中。

然而，ICANN 组织缺乏相关资源或授权，难以核实所有提供这些用品的网站是否合法。

请帮助我们在您所在的区域保护互联网免受涉及 COVID-19 的恶意软件和网络钓鱼带来的影响。

您是一名医疗保健提供者、财务经理、政府监管人、政策制定者、公共安全官员或安全领域专家吗?

我们需要您的帮助!

以下是我们如何共同保护互联网用户免受 DNS 安全威胁的方式:

第 1 步
请使用您的母语和字符集列出涉及 COVID-19 疫情的、在您的区域正在使用或有可能被用来攻击个人或机构的词汇。

第 2 步
请将您列出的清单发送至 **octo@icann.org**，并在邮件主题栏中写上: **DNSTICR Term Suggestion（DNSTICR 专有名词建议）**

请在电子邮件正文部分每行列出一条您提交的新建议。

例如:
专有名词 1
专有名词 2

如果这些专有名词需要解释，请在您的专有名词清单后添加解释。

了解域名系统安全威胁信息搜集和报告 (DNSTICR) 项目，以及您可以做出怎样的贡献，使互联网变得更加安全！

了解更多信息
敬请访问 DNSTICR 专属网页：
https://www.icann.org/dnsticr

探索
了解 ICANN 组织在缓和 DNS 安全威胁方面所做的努力：
https://www.icann.org/dnsabuse

缩略语和专有名词
请点击下方链接，通过 ICANN 的缩略语和专有名词功能，阅读更多有关本指南中使用的缩略语和专有名词的信息：
https://go.icann.org/acronyms

域名
域名标签
域名系统 (DNS)
互联网协议 (IP)
互联网协议地址
第 4 版互联网协议 (IPv4)
第 6 版互联网协议 (IPv6)

联络我们

https://icann.org
flickr.com/icann
@icann
linkedin.com/company/icann
facebook.com/icannorg
soundcloud.com/icann
youtube.com/icannnews
instagram.com/icannorg

或访问我们的专属社交媒体页面：
https://go.icann.org/socialmedia