《统一域名争议解决政策》域名争议中的网络钓鱼索赔

针对网络犯罪潮的回应

#GLPoint

Davide L. PETRAZ
Co-Managing Partner

Tommaso LA SCALA
Trademark Attorney

DNS（域名系统）和 UDRP （统一域名争议解决政策）正经历着 90 年代后期未曾见过的数字环境。

当商业互动与交易从纸质转换到数字世界，且随着软件设计工具出现并对大部分公众而言成为主流，网络犯罪也随之大幅增长，也因此对知识产权权利人造成巨大损失。金融诈骗、盗用身份和盗取有价值的商业信息等也只是对 UDRP 程序产生重大影响的众多剥削性行为中的一部分。

众所周知，网络钓鱼是一种用于盗取包括登陆账户密码和信用卡账号等用户信息的社会工程攻击。

近年来，网络钓鱼技术迅速从传统的 "模仿 "企业官方网站/邮件/账单等演变为更精炼的方法，其中 "鱼叉式网络钓鱼 "就值得单独写一篇论文。

鱼叉式网络钓鱼是一种涉及高度个性化引诱内容的有针对性的网络钓鱼攻击。攻击者通常会通过调查意向目标的社交媒体和对其他信息源进行侦察。这种做法可能涉及引诱网络用户登陆假冒网站并泄漏账户密码。还可能诱使用户点击链接打开文件而自动安装恶意软件。攻击者则可以通过恶意软件远程操控被感染的电脑。

根据 Verizon 发布的《2021 数据泄露调查报告》（DBIP），在美国，有 74%的组织遭遇过网络钓鱼攻击，其中 96%通过电子邮件发送。金融、电子商务以及零售等行业更容易成为这类攻击的目标。

即便大多数情况下电子邮件是这些网络钓鱼攻击的主要载体，至少令人欣慰的是 UDRP 是反击网络诈骗的一个有力武器。事实上，电子邮件地址是“域名”的一种，属于 UDRP 的管辖范围，除此之外，UDRP 政策第 4(b)(iv)条款还涵盖了作为转移目的地的“其他在线网址”。

上述条款还包含了通过使用具有混淆性的相似域名在商标所有人与在线网址的电子邮件发送者之间建立虚假从属关系的方式。第 4(b)条非详尽列举的范围显然包括使用欺骗性的电子邮件域名来实施（或意图实施）欺诈。就此而言，消极持有域名（已注册但不在活跃的网站中积极使用）并不改变这种情况，原因在于专家组仍是根据《WIPO 综述》3.0 （3）中载明的标准和因素来判断是否缺乏合法正当性，即(i)投诉人标识的显著性程度和知名度，(ii)被投诉方未答辩或未提交任何实际善意使用或计划善意使用的证据，(iii)被投诉方隐瞒其身份或使用虚假的联系方式（违反注册协议），以及(iv)善意使用该域名的可信度不高。

WIPO 专家组建立的判例法似乎证实，域名注册人利用欺骗性的电子邮件域名实施欺诈（如虚假的供应商账单）的案件通常是 "简单明了的"：事实上，诈骗在类型上的差异通常不会影响裁定结果。考虑到前述所有情况，尽管单一的 UDRP 程序不会对非法注册活动的数量产生重大影响，但毫无疑问，它们代表着品牌所有者可以通过这个快速同时兼具成本效益的工具，以阻止诈骗者在网上实施极具破坏性的行为。

Via L. Manara 13
20122 MILANO
Tel: +39 02 54120878
Email: glp.mi@glp.eu

Viale Europa Unita 171
33100 UDINE
Tel: +39 0432 506388
Email: glp@glp.eu

Via di Corticella 181/4
40128 BOLOGNA
Tel: +39 051 328365
Email: glp.bo@glp.eu

glp.eu

Other offices:
PERUGIA · ZÜRICH
SAN MARINO