域名系统攻击常见问题解答

（参考资料：ICANN 公告，2019 年 2 月 22 日）

问：为什么 ICANN 现在发布公告？
答：从媒体报道和安全专业人士提供的报告中，ICANN 已经了解到 DNS 正遭受攻击。因此，我们认为有必要采取措施，通过发布公告确保 ICANN 社群和一般会员公众了解事态的具体情况。这种做法符合我们自身的使命，即，确保域名系统 (DNS) 的安全性和稳定性。

问：DNS 遭受了哪种类型的攻击？
答：公共报告指出，有人正采取多种方法实施多层面的攻击。其中某些攻击是针对 DNS 的。通过对域名授权架构进行非授权更改，导致某些服务器地址被替换成由攻击者所控制的计算机地址。针对 DNS 的这种特定类型的攻击，仅在未部署域名系统安全扩展 (DNSSEC) 技术的情况下才能发挥威力。

问：攻击活动的幕后主使是谁？
答：有关攻击活动的幕后主使存在着相互冲突的报导，而且通常很难具体确定操纵此类攻击的真正主体。

问：执法机构是否正在调查攻击活动？
答：公共报告指出，多个国家或地区的执法机构和国家安全机构已对攻击活动展开调查。同时，公民社会（域名系统工程师、网络安全专家及其他相关人士）也正积极努力，以确定所使用的攻击类型。他们还协助受影响的组织强化系统。

问：ICANN 系统是否遭到攻击？
答：没有迹象表明 ICANN 系统遭到攻击。为谨慎起见，我们已经对 ICANN 系统进行了全面审核。

问：是否有任何根服务器遭到攻击？
答：没有迹象表明任何 DNS 根服务器遭到攻击。ICANN 已经联系了根服务器系统咨询委员会 (RSSAC)，要求其与根服务器运营商沟通，以确认没有 DNS 根服务器遭到攻击。截至目前，我们没有收到任何根服务器运营商发来的已检测到危害的通知。

问：遭受攻击的风险有多大？有多少域名是不安全的？
答：部分攻击利用了已遭感染的密码。我们没有办法知道还有多少密码已遭感染。因此，我们再次呼吁 DNS 生态系统内的所有方：务必使用强密码并定期更改，切勿在多个站点中重复使用相同密码，同时尽可能地使用多重要素验证。

问：攻击活动是否仍在继续？是在什么时候开始的？将会在什么时候终止？
答：尽管我们不知道攻击活动是否仍在继续，但是我们认为风险持续存在。我们建议所有组织务必提高在线安全性，包括实施域名系统安全扩展 (DNSSEC) 技术（如果还未实施的话）。此外，所有组织还应确保他们的域名管理使用强凭证，并审核系统是否存在遭受感染或篡改等的迹象。已发布的报告显示，这一系列的攻击活动最早始于 2017 年。

问：ICANN 是否有推荐任何具体措施？

答：有，ICANN 在 2019 年 2 月 15 日发布了一份核对清单，尽管此清单无法涵盖应该实施以确保系统安全的所有措施：

- 确保所有系统的安全补丁均已得到审核和应用
- 审核未经授权的系统访问活动的日志文件，特别是管理员的访问
- 审核对管理员（“根”）访问的内部控制
- 验证每条 DNS 记录的完整性，以及这些记录的变更记录
- 使用足够复杂的密码，特别是增加密码的长度
- 确保不与其他用户共享密码
- 确保永远不会以明文形式保存或传输密码
- 确保定期更改密码
- 执行密码锁定策略
- 确保 DNS 区记录均已获得 DNSSEC 签名，且您的 DNS 解析器能够执行 DNSSEC 验证
- 最好能够确保所有系统均采用多重要素验证，特别是针对管理员的访问
- 最好能确保您的电子邮件域采用符合 SPF 和/或 DKIM 标准的 DMARC 策略，且您能够在自己的电子邮件系统中执行其他域提供的这类策略

问：实施 DNSSEC 是否有助于保护最终用户安全？

答：是。实施 DNSSEC 有助于保护用户免遭特定类型的攻击。某些用于挂载攻击的系统使用了受 DNSSEC 保护的域名，此类 DNS 区的所有者证实，使用 DNSSEC 有助于抵御攻击。