采取措施从两大方面阻止域名劫持 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/252/2021_2022__E9_87_87_E5_8F_96_E6_8E_AA_E6_c101_252823.htm 简单来说，域名劫持就是把原本准备访问某网站的用户，在不知不觉中，劫持到仿冒的网站上，例如用户准备访问某家知名品牌的网上商店，黑客就可以通过域名劫持的手段，把其带到假的网上商店，同时收集用户的ID信息和密码等。 这种犯罪一般是通过DNS服务器的缓存投毒（cache poisoning）或域名劫持来实现的。最近几个月里，黑客已经向人们展示了这种攻击方式的危害。今年3月，SANS Institute发现一次将1,300个著名品牌域名改变方向的缓存投毒攻击，这些品牌包括ABC、American Express, Citi和Verizon Wireless等；1月份，Panix的域名被一名澳大利亚黑客所劫持；4月，Hushmail的主域名服务器的IP地址被修改为连接到一家黑客粗制滥造的网站上。跟踪域名劫持事件的统计数据目前还没有。不过，反网页欺诈工作组(APWG)认为，这一问题已经相当严重，该工作组已经把域名劫持归到近期工作的重点任务之中。 专家们说，缓存投毒和域名劫持问题早已经引起了相关机构的重视，而且，随着在线品牌的不断增多，营业额的不断增大，这一问题也更加突出，人们有理由担心，骗子不久将利用这种黑客技术欺骗大量用户，从而获取珍贵的个人信息，引起在线市场的混乱。 虽然，域名劫持在技术上和组织上解决起来十分复杂。但是在目前情况下，我们还是可以采取一些措施，来保护企业的DNS服务器和域名不被域名骗子所操纵。 破解困境 DNS安全问题的根源在于Berkeley Internet Domain (BIND)

。BIND充斥着过去5年广泛报道的各种安全问题。VeriSign公司首席安全官Ken Silva说，如果您使用基于BIND的DNS服务器，那么请按照DNS管理的最佳惯例去做。 SANS首席研究官Johannes认为：“ 目前的DNS存在一些根本的问题，最主要的一点措施就是坚持不懈地修补DNS服务器，使它保持最新状态。 ”Nominum公司首席科学家、DNS协议原作者Paul Mockapetris说，升级到BIND 9.2.5或实现DNSSec，将消除缓存投毒的风险。不过，如果没有来自BlueCat Networks、Cisco、F5 Networks、Lucent和Nortel等厂商的DNS管理设备中提供的接口，完成这类迁移非常困难和耗费时间。一些公司，如Hushmail，选择了用开放源代码TinyDNS代替BIND。替代DNS的软件选择包括来自Microsoft、PowerDNS、JH Software以及其他厂商的产品。 不管您使用哪种DNS，请遵循以下最佳惯例： 1. 在不同的网络上运行分离的域名服务器来取得冗余性。 2. 将外部和内部域名服务器分开（物理上分开或运行BIND Views）并使用转发器（forwarders）。外部域名服务器应当接受来自几乎任何地址的查询，但是转发器则不接受。它们应当被配置为只接受来自内部地址的查询。关闭外部域名服务器上的递归功能（从根服务器开始向下定位DNS记录的过程）。这可以限制哪些DNS服务器与Internet联系。 3. 可能时，限制动态DNS更新。 4. 将区域传送仅限制在授权的设备上。 5. 利用事务签名对区域传送和区域更新进行数字签名。 6. 隐藏运行在服务器上的BIND版本。 7. 删除运行在DNS服务器上的不必要服务，如FTP、telnet和HTTP。 8. 在网络外围和DNS服务器上使用防火墙服务。将访问限制在那些DNS功能需要的端口/服务上。让注册商承

担责任 域名劫持的问题从组织上着手解决也是重要的一环。不久前，有黑客诈骗客户服务代表修改了Hushmail的主域名服务器的IP地址。对于此时，Hushmail公司的CTO Brian Smith一直忿忿不已，黑客那么容易就欺骗了其域名注册商的客户服务代表，这的确令人恼火。 Smith说：“ 这件事对于我们来说真正糟透了。我希望看到注册商制定和公布更好的安全政策。但是，我找不出一家注册商这样做，自这件事发生后，我一直在寻找这样的注册商。 ”Nominum公司首席科学家、DNS协议原作者Paul Mockapetris说，升级到BIND 9.2.5或实现DNSSec，将消除缓存投毒的风险。不过，如果没有来自BlueCat Networks、Cisco、F5 Networks、Lucent和Nortel等厂商的DNS管理设备中提供的接口，完成这类迁移非常困难和耗费时间。一些公司，如Hushmail，选择了用开放源代码TinyDNS代替BIND。替代DNS的软件选择包括来自Microsoft、PowerDNS、JH Software以及其他厂商的产品。不管您使用哪种DNS，请遵循以下最佳惯例： 1．在不同的网络上运行分离的域名服务器来取得冗余性。 2．将外部和内部域名服务器分开（物理上分开或运行BIND Views）并使用转发器（forwarders）。外部域名服务器应当接受来自几乎任何地址的查询，但是转发器则不接受。它们应当被配置为只接受来自内部地址的查询。关闭外部域名服务器上的递归功能（从根服务器开始向下定位DNS记录的过程）。这可以限制哪些DNS服务器与Internet联系。 3． 可能时，限制动态DNS更新。 4． 将区域传送仅限制在授权的设备上。 5． 利用事务签名对区域传送和区域更新进行数字签名。 6． 隐藏运行在服务器上的BIND版本。 7． 删除运行在DNS服务器

上的不必要服务，如FTP、telnet和HTTP。 8. 在网络外围和DNS服务器上使用防火墙服务。将访问限制在那些DNS功能需要的端口/服务上。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com