

---

2009 年 8 月 19 日

## SAC 40: 防止域名注册服务遭到 非法利用或滥用的保护措施

ICANN 安全与稳定咨询委员会 (SSAC) 报告

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

## 序言

本报告由安全与稳定咨询委员会 (SSAC) 提供，旨在阐述防止滥用注册服务的一些保护措施。SSAC 负责针对互联网名称和地址分配系统的安全性和完整性向 ICANN 机构群体和理事会提供有关问题的建议。这包括运作问题（例如与正确、可靠地运行根域名系统有关的问题）、管理问题（例如与地址分配和互联网号码分配有关的问题）以及注册问题（例如与注册管理机构和注册服务商提供的诸如 WHOIS 之类服务有关的问题）。SSAC 一直从事互联网名称和地址分配服务的威胁评估和风险分析工作，评估哪里存在严重的稳定性和安全性威胁，并据此向 ICANN 机构群体提供建议。SSAC 不享有监管、强制执行或裁定的职权。这些职能属于其他机构，对于本报告中列出的建议，应根据建议自身的价值予以客观的评估。

本报告末尾列出本报告的编著者、关于委员会成员个人简介和利益声明的参考文档以及委员会成员对报告中各项调查结论或建议的反对意见。

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

# 引言

针对域名注册帐户的攻击和针对域名系统 (DNS) 配置的恶意篡改已成为危害网络安全的恶性事件。去年发生的一些事件证明了 DNS 和域注册帐户的访问权限仍然是攻击者的攻击目标。未经授权地修改与域名注册有关的信息 (包括恶意篡改 DNS 配置信息以便利用 DNS 将通信 (即使只是临时性地) 转发到原目标主机之外的目的地) 会严重扰乱商业运作并给组织带来经济和声誉上的损害。

无论是域名注册帐户劫持还是域名解析服务劫持, 都不是什么新的攻击手段。在过去的报告和建议中, ICANN 安全与稳定咨询委员会 (SSAC) 已经从用户 (注册服务商的客户, 即注册人) 的角度研究了影响域名注册和 DNS 运作的各种问题。我们已经发现有些注册人并没有采取足够的域名保护措施 (例如没有续订域名注册合同或者未能准确地维护联系信息)。我们已向注册人提供了保护与其注册和管理的域名有关的业务和运营利益的建议措施。

本报告提到最近发生的几起与未经授权而访问域注册账户有关的事件。提及这些事件并非要批评注册服务商、转销商或注册人, 也不是要另其难堪。我们这样做仅仅是因为, 针对安全事件的分析结果总是表明, 各方原本可以通过采取某些措施来避免发生这样的事件或者至少降低事件的危害程度。

在本报告中, 我们列举了几件与域名注册帐户有关并且引起广泛影响的事件, 此举的目的是想探讨这些事件的背后是否存在共同的起因, 这些起因是否昭示出了可以减少或减轻特定威胁和漏洞的有效措施。为查明攻击者如何取得域名注册帐户的控制权、随后又会执行哪些操作以及由此引发的种种后果, 本报告深入调查了这些事件的相关细节。关于这些事件的描述均摘自公开发表的新闻报道和文章。除此之外, 我们还补充了通过采访相关注册服务商及其客户而获得的信息。我们特意删除了相关方所认为的敏感信息。

本报告介绍了其他互联网商务行业 (例如金融、耐用品批发) 为防止攻击者利用类似的漏洞损害其客户的利益而采取的安全措施。本报告指出注册服务商可与客户交流经验, 双方联手保护已注册的域, 防止其遭到非法利用或滥用; 同时还讨论了如何增强注册服务商的风险意识, 并且指出即使只是暂时失去域名和相关 DNS 配置的控制权, 也可能会带来极大的风险。虽然有些注册服务商确实以其高水平的服务在域名注册市场中脱颖而出, 但本报告的目的是力图鼓励更多的注册服务商考虑是否有机会提供更多的保护措施来防止域注册帐户受到攻击。本报告还力图鼓励注册服务商将注册安全措施作为其在激烈的竞争市场中提供差异化服务的一种方法而予以重点考虑。

本文档译自英文版本, 旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性, 但英语是 ICANN 的工作语言, 本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿:  
<<http://www.icann.org/committees/security/sac040.pdf>>.

## 本报告的动机

过去十二个月中发生了几起与未经授权而访问域名帐户有关且引起广泛影响的攻击事件。这轮攻击风暴与之前促使 SSAC 针对域名劫持<sup>1</sup> 问题以及由于未续订域名而引起的意外后果而展开研究的事件具有一些共同之处。<sup>2,3</sup> 其中，有些事件是针对注册服务商工作人员和注册服务（例如支持 Web 的域帐户管理工具）的恶意行为。有些事件则是采用社会工程攻击技术，可能利用到了注册服务商与其客户之间的日常往来和通信特点。<sup>4</sup>

SSAC 针对 2008 年 5 月到 2009 年 4 月期间发生的一系列事件展开了深入的分析。通过这些分析，我们发现了一些常被攻击者利用的漏洞以及（业务和运作方面的）策略和习惯做法，并试图从中找出这些事件背后可能存在的一些共同点。我们在研究这些事件时注意到以下几点。

- (1) 许多组织的域名注册帐户都包含高价值或对业务至关重要的域名，对这些组织而言，这些域名可能会像组织所拥有的任何有形资产、商标或知识产权一样具有宝贵的价值。
- (2) 许多注册服务运营商的服务对象是消费者，换言之，其注册服务高度自动化，力求以很高的交易速率为众多的注册人提供服务。对于任何力求及时、可伸缩地提供服务的业务而言，自动化极为重要。我们的研究表明：攻击者已经熟悉注册服务商的行为并将利用自动化的某些特性发起攻击；例如，由于知道电子邮件是注册服务商向注册人通知联系方式和配置变更、续订等事宜的首选方法，攻击者便经常试图通过修改 DNS 配置来中断电子邮件的投递。
- (3) 在我们研究的事件当中，受害者往往是这样的客户：他们的域帐户对自身的业务非常重要，而代其运作这些域帐户的注册服务运营商又以消费者为主要服务对象。有些案例中，客户在成为受害者之前并没有充分意识到由于可能无法控制或访问其域注册帐户所带来的风险；另外一些案例中，客户在事件发生之前实施的内部策略和监控活动并不足以检测或阻止攻击。

---

<sup>1</sup> SAC007, Domain Name Hijacking Report:  
<http://www.icann.org/announcements/hijacking-report-12jul05.pdf>

<sup>2</sup> SAC011, Problems caused by non-renewal of a domain name associated with a DNS name server:  
<http://www.icann.org/committees/security/renewal-nameserver-07jul06.pdf>

<sup>3</sup> SAC010, Renewal Considerations for Domain Name Registrants: <http://www.icann.org/committees/security/renewal-advisory-29jun06.pdf>

<sup>4</sup> SAC028, Advisory on Registrar Impersonation Phishing Attacks (2008 年 5 月 26 日):  
<http://www.icann.org/committees/security/sac028.pdf>

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

部分受害者（取决于其规模和企业声誉）似乎在内部安全管理和风险管理方面颇有经验，能够意识到其域名的资产价值，然而，他们似乎并没有将域名列入风险评估的范畴之内。其他受害者，尤其是中小型组织或个人，在出现问题之前可能并没有完全认识到域名的重要性。这一点与组织或个人针对其他资产风险所采取的行为相同。许多情形下，组织可能认识到某项资产的价值或对业务的重要意义，但在发生事故之前并没有提供充分的保护措施来防止资产受到威胁。

从安全的角度来看，将域名视为重要资产的注册人在选择注册服务运营商时应将安全性作为一项重要的选择标准。SSAC 研究的事件表明，注册人要么不了解注册服务运营商提供哪些安全服务，要么并没有充分意识到有一系列的安全服务可供选择。有一家注册服务商曾向 SSAC 表示：注册人往往认为各个注册服务商的注册服务大体相同，其结论是既然所有的注册服务运营商都在销售来自同一注册管理机构的相同产品，那么注册服务商提供的安全措施也应该是相同的。我们在下一节中介绍的事件使 SSAC 得出了这样的结论：除域名机构群体之外，公众对注册服务运营商之间的差异尚缺乏充分的认识。

## 针对域名注册帐户的攻击

尽管列出与本主题相关的完整事件列表不是本报告的目的所在，但为了给后续的讨论和分析提供背景信息，我们还是列出了一些引起广泛影响、针对域名注册帐户的攻击事件的摘要信息。虽然这些摘要引自公开刊物，SSAC 还是征询了事件所涉注册服务商以及受害组织的意见并得到了他们的认可和配合。

### Comcast (2008 年 5 月)

Comcast 是美国最大的有线电视运营商、第二大互联网服务提供商和最大的固定电话运营商之一。<sup>5</sup>事件发生时，Comcast 已经通过 Network Solutions, Inc. 注册了大约 200 个域名。<sup>6</sup>2008 年 5 月 28 日，攻击者获得了由 Network Solutions 托管的 Comcast 域注册帐户的访问权限。最初，大概是想出风头，攻击者恶意修改了一些联系信息。<sup>7</sup> Comcast 工作人员收到关于联系信息更改的电子邮件通知后恢复了正确的信息。

攻击者声称他们曾要求一名 Comcast 管理员透露漏洞，然后他们便利用了这个漏洞。攻击者声称已经采用社会工程和技术攻击相结合的手段获得 Comcast 域注册帐户的访问权限。<sup>8</sup> Network Solutions 报告称不存在任何安全漏洞，他们的工作人员也没有可被利用的人性弱点，篡改

---

<sup>5</sup> 摘自 [en.wikipedia.org/wiki/Comcast](http://en.wikipedia.org/wiki/Comcast) 的 Comcast 条目

<sup>6</sup> Comcast.net Domain Hijacked at Network Solutions: <http://www.domainnamenews.com/featured/comcastnet-domain-hijacked-at-network-solutions/1619>

<sup>7</sup> How was Comcast.net hacked?: <http://blogs.zdnet.com/security/?p=1224>

<sup>8</sup> Comcast.net name hijacked: <http://www.internetidentity.com/2008/June-2008.html>

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

DNS 的是某些掌握客户登录信息的人。<sup>9</sup> *Wired Magazine* 杂志上刊登的一篇文章中表示：攻击者声称有一位 Comcast 经理“对他们的要求嗤之以鼻并且粗暴地挂断电话”。<sup>10</sup> 攻击者于是再度入侵该帐户。这次，他们篡改了 comcast.net 域的 DNS 配置并将通信重定向到一个恶搞网站，托管该网站的服务器此前已被他们攻陷。不过，Comcast 工作人员并没有收到 Network Solutions 关于配置更改的电子邮件通知。域注册记录中记录的技术人员和管理人员联系方式所使用的电子邮件地址均分配自 Comcast 已注册的域。通过篡改 DNS 配置，攻击者有效地避免了 Comcast 工作人员收到关于帐户活动的电子邮件通知：直接让这些电子邮件通知无法投递。这次攻击取得了成功并且登上全球媒体的头条。根据 *Wired Magazine* 的报道，“这次攻击大约从东部时间上午 11 点开始，直到下午四五点之前，攻击者一直掌控着 Comcast.net。即使在 Comcast 夺回控制权之后，仍然费时很久才让更改传播到整个 DNS，部分客户直到周四上午 11:30 都无法访问 Webmail。”2008 年 5 月 29 日 *The Register* 刊登的一篇文章中评论称“这次攻击表明即使是老套的帐户入侵方法也足以改变庞大的 Web 通信”。<sup>11</sup>

## CheckFree (2008 年 12 月)

CheckFree (如今更名为 FIServ) 是全球金融服务行业信息管理和电子商务系统的领导厂商。<sup>12</sup> 2008 年 12 月 2 日，一名攻击者获得了由 Network Solutions 托管的 CheckFree 域注册帐户的控制权。<sup>13</sup> 该攻击者修改了几个域 (包括 checkfree.com 和 mycheckfree.com) 的 DNS 配置。尝试登录帐户以使用在线账单支付服务的客户被重定向到了一个位于乌克兰的仿冒 Web 服务器，该服务器试图安装包含 Adobe Reader Exploit 的恶意代码。<sup>14</sup> CheckFree 在攻击之后的 8 小时内恢复了正确的 DNS 配置，但与其他类似的事件相同，在全球 DNS 基础架构中传播更改花费了更多的时间。<sup>15</sup>

华盛顿邮报 (*Washington Post*) 的“Security Fix”博客中指出，该攻击者通过正确的登录信息取得该帐户的访问权限。同一篇文章称，Network Solutions 强调攻击者并没有攻破其系统来获取登录凭据。<sup>16</sup> 攻击者究竟如何获得用户帐户和登录凭据，至今仍不清楚 (或者尚未披露)。

---

<sup>9</sup> Comcast account access issue – clarification:  
<http://blog.networksolutions.com/2008/comcast-account-access-issue-clarification/>

<sup>10</sup> Comcast Hijackers Say They Warned the Company First: <http://blog.wired.com/27bstroke6/2008/05/comcast-hijacke.html>

<sup>11</sup> Potty-mouthed hackers steal comcast.net keys, go for a spin:  
[http://www.theregister.co.uk/2008/05/29/comcast\\_domain\\_hijacked/](http://www.theregister.co.uk/2008/05/29/comcast_domain_hijacked/)

<sup>12</sup> FIServ: <http://en.wikipedia.org/wiki/Fiserv>

<sup>13</sup> DNS attack hijacks payment website: <http://www.techworld.com/security/news/index.cfm?newsid=107959>

<sup>14</sup> Network Solutions phishing attack preceded CheckFree domain takeover:  
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9122722>

<sup>15</sup> <http://www.internetidentity.com/2008/Nov-Dec-2008-FIN.html#cf>

<sup>16</sup> Digging Deeper into the CheckFree attack:  
[http://voices.washingtonpost.com/securityfix/2008/12/digging\\_deeper\\_into\\_the\\_checkf.html](http://voices.washingtonpost.com/securityfix/2008/12/digging_deeper_into_the_checkf.html)

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

## ICANN、Photobucket、Photobucket (2008 年 6 月)

2008 年 6 月 26 日, ICANN 自己也成为一个黑客组织的牺牲品, 该组织非法取得了由 Register.com 托管的 ICANN 域注册帐户的访问权限。根据 ICANN 的新闻发布稿, 这次攻击“组织严密, 结合使用了社会工程攻击知识和技术手段”<sup>17</sup>。根据 ICANN IT 总监的介绍, 攻击者篡改了几个域 (icann.net、iana-servers.com、icann.com、internetassignednumbersauthority.com 和 iana.com) 的 DNS 配置, 导致访问者在访问这些域时被重定向到一个以免费 Web 托管帐户 (该帐户由 Atspace.com 运作) 发布的恶搞网站。有人根据此次事件的发生时间 ICANN 巴黎会议的开始日期, 此次会议举行了关于新 GTLD 的公开讨论) 和恶搞消息自身推测此次攻击基于政治目的。ICANN IT 工作人员检测到 DNS 更改后通知了 Register.com, 后者收到通知后很快恢复了正确的配置信息。然而, 与 Comcast 事件中的情形相同, 在更正后的信息向全球传播的过程中, 篡改的 DNS 配置信息据估计仍然在全球 DNS 中保留了 24 到 48 小时<sup>18</sup>。

声称对 ICANN 攻击事件负责的黑客组织在随后的攻击中也采用了类似的伎俩和相同的免费 Web 托管服务商。Photobucket 是 Fox Interactive Media 于 2007 年收购的一家图像托管、视频托管、幻灯片和照片共享网站。<sup>19</sup> 2008 年 6 月 18 日, 这个黑客组织声称对针对 Photobucket 的攻击行为负责, 这次攻击导致对 Photobucket 用户的服务中断。<sup>20</sup> 2009 年 2 月 7 日, 该组织又对成人素材托管网站 RedTube 实施了另一次恶搞性攻击。<sup>21</sup> <sup>22</sup>

## DomainZ (2009 年 4 月)

DomainZ (Domainz.net.nz) 是 MelbourneIT 设在新西兰的分公司, 也是一家注册服务商。2009 年 4 月 21 日, 有好事之徒通过对 DomainZ 的密码检索页面执行结构化查询语言 (SQL) 注入攻击收集了几个知名的注册人 (包括 Coca-Cola、Fanta、F-secure、HSBC、Microsoft、Sony 和 Xerox) 的帐户凭据。攻击者修改了 .CO.NZ 下注册的域的 DNS 配置记录, 使之指向 .INFO 域下的已注册域名服务器 (turkguvenligi.info)。这些服务器存放了未经授权的区域信息, 此信息会将遭到攻击的域解析到由攻击者托管的恶搞网站。其中一部分访问量进入以该品牌名称 (例如 Microsoft) 为恶搞对象的恶意网站, 另一部分流量则被重定向到政治抗议页面。

---

<sup>17</sup> ICANN Response to Recent Security Threats: <http://www.icann.org/en/announcements/announcement-03jul08-en.htm>

<sup>18</sup> Turkish criminal hackers hijack ICANN sites: [http://news.cnet.com/8301-10789\\_3-9980713-57.html](http://news.cnet.com/8301-10789_3-9980713-57.html)

<sup>19</sup> Photobucket: <http://en.wikipedia.org/wiki/Photobucket>

<sup>20</sup> Photobucket's DNS records hijacked by Turkish hacking group: <http://blogs.zdnet.com/security/?p=1285>

<sup>21</sup> Popular porn site attacked by prudes: <http://www.securecomputing.net.au/News/102818.popular-porn-site-hacked-by-prudes.aspx>

<sup>22</sup> Turkish Hackers Take Out Top Porn Site:  
<http://www.darkreading.com/security/perimeter/showArticle.jhtml;jsessionid=FV31FLACFRJQYQSNLPSKH0CJUNN2JVN?articleID=208803672&subSection=Security>

本文档译自英文版本, 旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性, 但英语是 ICANN 的工作语言, 本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿:  
<<http://www.icann.org/committees/security/sac040.pdf>>.

## 这些事件有何启示？

Comcast、ICANN、Photobucket 和 RedTube 攻击事件之间的相似之处说明了域注册帐户攻击者对 Web、文件传输和其他互联网应用程序执行攻击时大都沿用相同的套路，即采用下述方式：一旦成功利用了某个漏洞，攻击者会继续沿用这套伎俩并扫描存在相同或相似漏洞的目标。

SSAC 从这些事件中注意到以下几点。

对于某些注册服务商：

1. 攻击者控制组织整个域名资产（并妨碍对该资产的合法访问）所需的只不过是用户帐户和密码。
2. 攻击者只需要猜测、仿冒或对某个联系人运用社会工程攻击技术，即可获得域注册帐户的控制权。
3. 攻击者扫描域注册帐户和管理门户以查找 Web 应用程序漏洞（例如 SQL 注入）。对存在漏洞的应用程序代码一旦攻击得手，可能会导致多个域帐户的帐户凭据遭到泄露。
4. 电子邮件是某些注册服务商向注册人通知帐户活动的的首选方法，甚至常常是唯一的方法。（我们将在后文讨论其他的联系方法）。
5. 攻击者可以通过篡改 DNS 配置信息阻止向目标注册人发送电子邮件通知，因此导致不会向攻击者通过已侵入的帐户控制的域中的任何收件人（例如该域中托管的、由注册人指定的管理或技术联系电子邮件地址）发送电子邮件通知。
6. 访问和修改某个注册帐户中所有域的联系信息和 DNS 配置信息的权限通常都通过某个用户帐户和密码进行授权。
7. 即使迅速发现了 DNS 信息遭到未经授权的修改，要将恶意配置的 DNS 信息恢复为正确的信息也很费时间，这是由 DNS 的分布式特性和 TTL 值所决定的。

## 客户对注册保护措施不够熟悉

某些注册服务商善于保障业务的安全和保护客户的利益。他们运用最佳的措施来保障 Web 应用程序、域名和托管服务器的安全。他们监控系统和帐户的可疑活动。注册服务商的支持人员能够有效地响应滥用或违法投诉。然而，在域注册服务大行其道的行业中，就像任何电子商场或在线商务一样，难免会有些注册服务商暴露出可被已知攻击手段利用的漏洞。其他行业中，即使是安全方面做得最好的组织，在遇到安全审核中没有考虑到或者组织从未遇到的攻击手段面前往往也表现得不堪一击。

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

从本报告中讨论的事件（以及 SAC012 中所引用的以及在其发布后所发生的其他类似事件）中可以清楚地看到：注册服务商的流程一直都是并将继续充当攻击者入侵的跳板。考虑到行业的规模和多样性，这种情况并不罕见。注册服务商一直都是、也将继续是攻击者的目标。就像金融机构的客户可能会成为针对在线银行门户的攻击的目标一样，域注册帐户也可能成为针对注册服务商管理页面的攻击的箭靶。

归根结底，如何评估针对域名和 DNS 配置的攻击的风险，以及如何选择注册服务使注册人遭受攻击的可能性降低到可接受的范围之内，都是注册人的责任。然而，注册服务商通常不会引导客户注意他们提供的保护措施，对如何比较针对域名注册的安全服务也是避而不提，因此，客户可能会误以为所有的注册服务商在安全方面都是一样的，因此在选择时显得比较盲目或漠不关心。

### 注册服务商有各自不同的目标市场和服务模式

考虑到这一点，SSAC 分析了各种域名注册服务并得出这样的结论：域名注册大体有两种服务模式。

比较流行的服务模式是提供最基本的域名注册服务，以便降低价格。服务的交付高度自动化，侧重于快速统一、可重复地大批量处理交易，这样常常可以将人为的错误减少到最低限度。与客户的通信通常通过电子邮件实现，这些电子邮件主要用于发送通知或传达简单的操作说明（常常是分步操作指导），以指导客户完成强制性的流程（例如，WHOIS 年度准确性审查流程）。这种服务模式常常通过问题跟踪系统实现自动化的故障投诉流程。自动化通常都胜过人工参与；大多数情况下，当自动化流程的执行不符合客户的预期或客户不理解时，或者当客户遇到自动化流程无法解决的问题或需要报告事件时，客户往往会寻求人工干预。通常，要防止域帐户和 DNS 配置遭到滥用，可以遵循下列安全措施：利用安全套接字层 (SSL) 的保护登录域帐户和管理域资产，在与该帐户相关联的 DNS 或联系信息被修改时发送电子邮件通知，隐私服务（受保护或受委派的 WHOIS 服务，如 SAC023 中所述<sup>23</sup>）以及域名迁移保护（注册服务商锁定、转出注册服务商和转入注册服务商之间的授权代码确认）。<sup>24</sup>

另一种注册服务模式提供保护措施，以满足如下客户的需求：对其域名赋予很高的价值、将其域名和网络影响力视为业务的关键因素、或者意识到其企业或品牌可能成为各种滥用行为或犯罪活动的追逐目标。这些客户意识到域名面临的威胁，希望尽可能地减少或降低域名丢失、配置错误、联系信息或 DNS 配置信息遭到篡改或域名遭到滥用的风险，他们已经为做出知情决策收集了足够的信息，能够挑选出满足这些要求的注册服务商。此类注册服务商提

---

<sup>23</sup> SAC023, Is the WHOIS Service a Source for email Addresses for Spammers?  
<http://www.icann.org/en/committees/security/sac023.pdf>

<sup>24</sup> 有些注册服务商实施防滥用安全措施来保护内部（业务关键型）系统、流程和数据库。这些对注册服务商的客户来说通常都是透明的。

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

供各种安全措施来防止由于技术错误或疏忽而导致客户无法续订域名，通过阻止未经授权地篡改注册记录防止客户的域名遭到劫持，并阻止未经授权的恶意 DNS 配置。这些注册服务商的业务模式注重于逐项处理单笔交易，力求将错误概率控制在非常低的限度内。此类注册服务商主要面向那些重视域资产保护、愿意为支持（特别是为客户分配帐户专员来提供支持）支付额外费用的客户。例如，客户可能希望具有这样的安全功能：在注册服务商对 DNS 配置和域名解析服务执行更改请求和实时监控之前，事先征得客户授权的联系人的口头或书面同意。

一般来说，在强调品牌权益保护的服务包中都包含上述措施。品牌权益保护措施力求降低各种风险，包括商标滥用（即未经授权地使用商标或品牌来吸引互联网用户访问商标/品牌持有人之外的网站）、针对品牌持有人（使用视觉上相似、“同形异义”的域进行仿冒或欺诈攻击）域注册、分食收入或流量、延后订单（试图代表某个客户抢注已被其他方注册的域、这些域随后会再度可用）以及防御性注册（在所有顶级域中注册一个商标或名称）。

### 谁需要防止域帐户和 DNS 劫持的保护措施？

一般来说，针对恶意篡改域帐户或 DNS 配置信息的强大保护措施，是那些在域资产或品牌权益方面投入巨资、愿意为保护其品牌支付额外费用的组织所熟悉且孜孜以求的。然而，注册人不要以为 *只有拥有需保护的的品牌或知识产权的公司才需要防止域帐户遭到劫持或 DNS 配置信息遭到恶意篡改的保护措施*。有许多组织，虽然网络影响力是决定成败的关键因素，但他们使用的域名可能与其品牌并无关联。还有些组织使用他们注册的任何域名都可以轻松地经营业务。但如果这类组织对其网页、邮件和其他互联网服务所使用的网络名称没有解析到他们托管这些服务所用的 IP 地址，他们将承受由此带来的损害或经济损失。

考虑到选择能够实质性降低与丢失域名或恶意篡改 DNS 配置信息有关的风险的注册服务商，确实能给有些组织带来益处，我们试图分析了这类组织在选择注册服务商时并未将安全措施作为其考虑因素的可能原因。下面是一些可能的原因：

**感知成本：**在有些案例中，组织主观或错误地认为：通过提供强大的域帐户和 DNS 反劫持保护措施的注册服务商来注册域名所需的成本将会高不可攀。

**认知度：**有些客户原本愿意为提供域帐户和 DNS 反劫持功能的强大保护措施买单，但他们却不知道有这样的服务存在。

**缺乏了解：**有些案例中，组织根据有限的信息推断出所有的注册服务商都采用大致相当的保护措施。

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

**“您的服务套餐并不适合我们公司”**：有些案例中，组织乐于为某些提供域帐户和 DNS 反劫持功能的强大保护措施买单，却不愿意或无力为（他们认为是）某些注册服务商捆绑提供的服务买单，例如在强大的保护措施之外提供品牌权益保护服务。

这里还有些问题值得讨论：

*是否只有寻求保护其品牌的组织才会对更强大的注册保护措施感兴趣？*

并非如此。许多组织既希望保护其品牌，也希望维护其网络影响力，但他们必须综合考虑需求与保护成本的平衡关系。强大的注册保护措施常常作为品牌权益保护的补充措施。注册服务商也许会在基本注册服务之外以选择性加入的服务或“付费”服务或两者兼而有之的形式提供强大的注册保护措施，对那些有意在安全措施上投资以降低由于非法利用或滥用导致注册域不可用的风险的组织来说，这些措施可以为他们提供所需的安全功能。

*除关注自身品牌的组织之外，其他组织在评估风险和管理资产时是否也应考虑域名事宜？*

是的。SSAC 报告已经阐述了在域名遭到劫持时注册人所面临的负面影响，包括财务损失、尴尬处境和声誉损害。<sup>25</sup> SSAC 报告还阐述了与未续订域名有关的事宜，以及由于未续订域名而引起的、与 DNS 名称服务器相关的问题。<sup>26</sup>特别是，SSAC 在 SAC010 中指出“域名应被视为具有市场价值的资产，无论是通过经纪人销售还是直接销售，或者应视为可带来重复性营收的一种手段”，“未续订（自愿或无意）注册域名的注册人应注意每个域名对某些人来说都具有潜在的价值…新注册人可能会使用失效的域名从事对原注册人不利的活动”。<sup>27</sup>

*可以向将域名视为重要资产的组织提供哪些保护性措施，来帮助他们管理风险并消除他们在域名方面以及依赖于域名的投资所面临的各种威胁？*

其他互联网商务行业（例如金融、耐用品电子商场）中采用的一些措施对保护注册服务也有帮助并有实际运用的价值。在考虑具体的措施之前，特别是从维护注册人利益的角度出发，

---

<sup>25</sup> SAC007: Domain Name Hijacking Report (2005 年 7 月 12 日) :  
<http://www.icann.org/announcements/hijacking-report-12jul05.pdf>

<sup>26</sup> SAC011: Problems caused by the non-renewal of a domain name associated with a DNS Name Server (2006 年 7 月 7 日) :  
<http://www.icann.org/en/committees/security/renewal-nameserver-07jul06.pdf>

<sup>27</sup> SAC010: Renewal Considerations for Domain Name Registrants (2006 年 6 月 29 日) :  
<http://www.icann.org/committees/security/renewal-advisory-29jun06.pdf>

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

有必要重新评估第一条原则：特别是如何将大型组织使用的资产、策略配置和风险管理框架运用到域名注册中？为何将域名注册视为一项资产？

之前的 SSAC 报告给出这样的解释：域名是实体（商家、金融机构或教育机构、赢利或非赢利组织或企业、个人或产品）在互联网上赖以成名或经营业务的标识。域名可与公司经营业务所用的名称 (DBA) 和名人、作者、政治人物或其他人士的姓名相同。个人和组织都会将现实世界中的名称（品牌、服务标识、商标）视为资产并采取措施防止（公司章程、专利、版权等遭到）滥用。域名常常与组织的品牌、服务标识、商标相同，因此，注册人应该采取措施来保护此类名称，不能仅仅注册名称，还需要防止遭到非法利用或滥用。

域名注册确保域的全球唯一性，并且只要注册人继续支付续订注册费用并遵守合同义务（例如合法使用域名、确保注册信息的准确性），域名将一直属于注册人所有。这与其他网络管理方法（例如资产、风险和策略控制）相似。

域名也是用户友好的标识符，可以使用 DNS 进行解析以确定为该域提供服务（Web、邮件、社交网络、语音...）的主机的互联网地址。域保持正常运行（特别是确保域名解析的高可用性和域名的正常解析）对大多数组织来说都具有不可估量的价值。

例如，在资产和风险管理计划中，可以：

- 确认（有形或无形）资产的价值；
- 列出该资产面临的威胁形式（损失、失窃、滥用）；
- 确定威胁是如何实现的，也就是说是什么原因导致域名易被攻击或利用？
- 确定每种威胁入侵的可能性或风险；
- 确定如何减轻或降低这种风险；
- 确定将风险减轻或降低到可接受的风险和成本所需的成本；以及
- 确定相应的预算并执行减轻或降低风险的措施。

如果承认域名是一项资产，那就应该像对待其他列入资产清单的、宝贵或敏感的资产一样予以严格保护。从这个角度来看，域名注册管理与大型网络中的策略控制管理似乎有许多共同之处。例如，策略控制和域名注册中的主要操作都是 {添加、丢弃、更改}。策略控制管理中应用的最好做法都是为了确保这些操作由授权方以可接受审查的方式及时而又有条不紊地执行，并且将出现各种疏忽、干扰或错误的可能性降低到极低的限度。在域名注册管理中也应当借鉴这些最佳做法，注册服务应当力求符合类似的最佳做法。

对组织来说，保护域名注册的安全措施应当与组织为内联网、远程数据库和其他应用程序访问提供的安全措施同等重要，后者通常被组织视为影响业务的关键因素。对于将域名注册视为具有重要价值的资产的客户来说，要尽量降低域名注册管理中出现疏漏、干扰或错误的可能性，应当实施与他们对其他业务关键型应用所实施的服务相仿的身份验证、授权和审核服

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

务。其中有些措施可由客户自行实施。其他措施可由注册服务商加入到注册服务中，倘若注册服务商决定提供附加安全措施，希望以此作为在竞争激烈的市场中突出自身优势的一种手段的话。我们将在后文详细讨论这些措施。

## 防止域帐户和 DNS 劫持的措施

本节中，我们将介绍当今部分注册服务商所提供的一些措施，这些措施是其广泛的服务中的一部分，常常与在线信誉（品牌权益）保护措施一起提供。接下来，我们要介绍的是：对于 SSAC 调研 2008 各大安全事件的过程中所采访的相关方面，注册服务商原本可以为他们提供哪些可取或基本的措施。最后，我们认真分析了大型企业为保护远程应用程序访问所采取的措施以及金融机构和电子商场为保护客户帐户所提供的措施。无论是作为自愿选择加入的服务还是作为一项服务套餐，对于希望降低非法利用或滥用域帐户的风险并愿意在相关的保护措施上投资的客户来说，提供的这些服务都可以帮助他们提高域注册帐户的安全性。我们鼓励注册服务商考虑提供这些措施是否可以为其在竞争激烈的市场中带来机遇或作为突出自身优势的一种手段。

客户（注册人）在保护域名方面扮演着关键的角色。本节中，我们简要地介绍客户可以且应采取的一些补充措施来 (a) 确保其在与创建和续订域注册帐户相关联的注册人-注册服务商工作流程中的角色安全性，以及 (b) 确保维护和更改联系信息和配置信息的流程安全性。注册服务商可以通过现有或新增的常见问题解答 (FAQ) 或其他方式向拥有非常重要的域资产的客户推荐这些措施。例如，我们鼓励注册服务商向客户分发本报告以让其了解相关的内容，鼓励客户阅读本报告并实施他们认为必要的措施来降低或减轻他们认为对其域名资产威胁最严重的风险。

SSAC 相信：对于中小型组织来说，与由各种孤立的举措和实施方案拼凑的组合方案相比，一款能够全方位迎合域注册帐户保护需求的服务方案会有更大的市场空间和压倒性的竞争优势。我们是根据对统一威胁管理 (UTM) 安全设备的成功的观察而做出上述推断的，UTM 是将防火墙、防垃圾邮件、防病毒和其他安全服务捆绑在一起的安全系统。与由各种性能虽属业界一流、但仅提供单一安全功能的安全系统组成的组合系统相比，这些全功能设备在中小型企业中具有更强的市场渗透能力，最终也取得了更大的成功。我们相信：对中小型企业来说，正如 UTM 那样，提供附加的安全措施会给域注册业务带来同样的影响。

## 保护对域资产的访问

本节中介绍的措施旨在防止通过注册服务商或转销商的在线 (Web) 用户界面或支持中心未经授权地访问客户的域名帐户。

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

注册验证。针对大批量交易和快速配置域名而优化的注册模式并不能很好地验证注册人所声称的身份是否属实，也不能验证支付过程中是否存在欺诈或犯罪行为。反钓鱼研究和<sup>28</sup>·<sup>29</sup>对付僵尸网络 (Srizbi, Conficker) 及 Fast Flux 攻击网络的经验表明域注册帐户现在是、将来也将继续是犯罪活动的重要资源。在注册人注册时以及每次修改联系信息时验证注册人提交的联系信息，可以降低仿冒和域名滥用的风险。我们鼓励服务注册商考虑提供电子邮件注册确认机制；只有在注册人通过访问注册服务商发送的激活电子邮件中嵌入的超链接来确认其电子邮件地址之后才完成域的注册流程。作为一项补充措施，有些金融机构会拨打客户提交的电话号码而不是使用电子邮件确认。公司通过电话提供确认码，客户在 Web 表单中键入此确认码以激活帐户或授权交易。SSAC 承认此类措施会延迟注册流程和产品交付（注册域名的注册和域名解析），但我们鼓励注册服务商将这一负面影响与降低域名滥用风险（不仅仅是为了客户，也是为了整个互联网普通用户群体）所带来的价值进行权衡考虑。另一项好处是：与安全性方面相对落后的其他注册服务商相比，在确保互联网域名系统的安全性方面明显领先同行的注册服务商，将会赢得更高的声望，也将赢得安全专家和业界同行更多的推荐。

**改进基于密码的身份验证系统。**目前，注册服务商最常用的身份验证方法是简单的用户名和密码。注册服务商并没有义务强制密码的最短长度、最长有效时间或复杂性检查，也没用通过限制不正确的登录尝试次数来应对暴力猜测攻击。上述措施是普遍接受的最佳安全策略，建议在任何基于密码的身份验证系统中都应采用这些措施。

**系统注册。**现在，电子商场和金融机构通过允许客户注册客户将来管理帐户所用的个人计算机 (PC) 或 IP 地址来提供改进的密码系统。

**多因子身份验证**电子商场、金融机构、甚至是在线（角色扮演）游戏运营商都允许客户选择增加硬件令牌验证密钥作为帐户登录期间验证客户身份的第二个因子。密码代表的是“您知道什么”，令牌则增加了“您有什么”这一条件。这种双因子身份验证使攻击者更难侵入域帐户：即使攻击者猜对或获悉帐户的登录名和密码，他还必须手中拿到令牌。如今有许多双因子身份验证方案，这种技术也有庞大的客户群。SSAC 注意到 VeriSign 已通过 ICANN 的注册管理机构服务评估流程 (RSEP) 提交了一份注册管理机构对注册服务商的双因子身份验证服务提案。该提案提出将“当前用于处理更新、迁移和/或删除申请所用的用户名和密码将通过动态验证码进行增强”作为注册服务商的一项自愿选择服务。<sup>30</sup> VeriSign 建议的部署方案的第一个阶段是在注册管理机构和注册服务商之间增加双因子身份验证机制。第二个阶段是为注册人对注册服务商的申请流程提供这种服务，包括在注册服务商到注册管理机构的可扩展策略控制协议 (EPP) 交易中使用一次性密码策略。SSAC 鼓励注册服务商阅读

---

<sup>28</sup> APWG 钓鱼活动趋势报告（2008 年下半年）：  
[http://www.antiphishing.org/reports/apwg\\_report\\_H2\\_2008.pdf](http://www.antiphishing.org/reports/apwg_report_H2_2008.pdf)

<sup>29</sup> Global Phishing Survey:Trends and Domain Name Use in 2H2008:  
[http://www.antiphishing.org/reports/APWG\\_GlobalPhishingSurvey2H2008.pdf](http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf)

<sup>30</sup> VeriSign Registry-Registrar Two-Factor Authentication Service: <http://www.icann.org/en/registries/rsep/>

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

此项提案并考虑实施此项提案有何益处。除了考虑上文提到的双因子身份验证之外，SSAC 建议注册服务商也可考虑各种身份验证方法和验证标准，例如美国标准和技术协会 (NIST) – 电子身份验证标准。<sup>31</sup>

**质询系统。**有些金融机构会在账户设置期间收集一组有关个人身份识别问题的答案。金融机构会从这些问题中随机选择一组问题并要求尝试登录账户的任何人作出回答。其他一些金融机构则会要求用户辨识机密图像-标题对。客户首次登录账户时必须选择一幅机密图像。然后提交图像标题。在验证流程中，客户在输入密码之前必须先提供与该图像匹配的标题。在保护域名和防止 DNS 配置滥用的方案中引入这种附加的质询机制会带来一定的成本和不便，我们鼓励注册服务商以自愿选择的服务形式为愿意接受这一点的客户提供这种安全措施。

**基于每个域的访问控制。**一旦拥有一个域注册帐户的访问权限，用户和攻击者就会对该帐户下注册的所有域拥有不受限制的访问权限。现实世界中经常遇到的与此类似的注册帐户访问模式是机柜模式的银行保险箱：一旦您打开这种机柜，您就可以随心所欲地打开其中的多个保险箱了。不妨比较一下这种模式的保险箱和包含保险箱的银行金库：对于后者，客户或入侵者不仅要进入金库，还必须获得每个保险箱的钥匙。我们鼓励注册服务商考虑为寻求更强大的保护措施的客户提供类似的 *访问模式*；例如，可以提供一种自愿选择的功能，允许客户控制哪些联系点可以更改联系信息和 DNS 确认信息、启动或授权域名迁移等。

**多个互不相同的联系点。**对组织来说，在域注册记录中维护准确的联系点信息是一件有益的工作。对某些组织来说，让每个必要的联系点均由组织内部专人或专职充当也很有好处。这样可以分散内部员工企图声称拥有域名所有权或试图从其雇主或雇主的客户手中攫取域名的风险。SSAC 建议希望防止域名遭到内部员工滥用的注册人考虑上述措施。这些措施还给需要为注册人管理联系信息的注册服务商提供了机会。例如，注册服务商可以要求和检查联系点信息（尤其是首选的通信方式，例如电子邮件地址）的唯一性并以此作为自愿选择的服务功能。注册人和注册服务商可以利用联系点唯一的特点建立细化的权限模式。例如，有些组织可能希望确保只有身为注册人的联系点可以迁移域名或者只有技术联系点可以更改 DNS 配置（这里只是举例说明，当然还存在其他模式）。注册服务商可以通过将这些措施与其他措施（例如交互式确认或多收件人通知流程）结合在一起鼓励注册人选择这些措施。

**更改通知或确认。**有些组织通过制定要求对特定操作进行多方确认的工作流程来防止未经授权或错误的更改。多方确认加强了组织对仿冒行为的防御能力：攻击者不能只是对某一方（而必须是对双方同时）执行社会工程攻击或仿冒攻击。有些组织可能有兴趣选择那些注册服务商要求提供多个独立的联系点且要进行检查的服务。这样，这些组织可以将他们内部使用的这种工作流程延伸到对联系点的更改、域名迁移或 DNS 配置上。对于没有这些工作流程的组织来

---

<sup>31</sup> [http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1\\_0\\_2.pdf](http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf)

说，注册服务商可以提供可选的服务以便代表客户实施这些工作流程。例如，在初次注册时，注册服务商的更改确认服务会检查客户是否已为与该域相关联的每个联系点提交唯一的联系人。更改确认还允许客户选择在申请更改 DNS 配置时必须通知哪些联系点，或者要求在执行单方申请的更改之前通过电话或电子邮件同时通知技术联系人和管理联系人。此外，更改确认还可帮助避免报复性或投机性的域名迁移。例如，请考虑如下情形：被指定为某个联系点的某位员工离开了该组织，该组织却忘记将联系信息从该员工更改为他的继任者。如果该员工是充满怨恨地离开组织，那么他可能会试图通过域名迁移获取域名所有权。在更改确认方案中，将会要求其他联系人确认域名迁移 该员工的迁移企图即会被阻止。

多收件人通知注册服务商通常使用电子邮件与客户联络。 SAC028 “仿冒注册服务商的钓鱼攻击” 中提到几种常见的通信类型，包括：

- 域名续订通知；
- 域名订购确认；
- 注册申请确认；
- 对域联系人信息和 DNS 信息的更改；
- WHOIS 数据准确性提醒；
- 通知域名过期或注销；以及
- 关于新服务和新功能的促销和广告

**提供向多个收件人发送此类函件的选项可给客户带来多方面的益处。**例如，客户可能希望避免成为仿冒注册服务商的钓鱼攻击的牺牲品：客户的某个收件人可能会误中钓鱼电子邮件的圈套，但另一位收件人则可能会识别出这是假冒的电子邮件并提醒注册服务商和他组织中的其他联系人。类似地，如果该注册服务商曾向多个收件人发送域名续订通知，则可避免出现由于客户失误或疏忽而导致注册失效的情形。例如，如果续订通知的唯一收件人正在休长假并且长时间没有查收电子邮件，那么续订可能会失效。在多收件人方案中，如果其他收件人收到了续订通知，就可以避免出现这种注册失效的情形。注册服务商也可以考虑借鉴某些金融机构协助其客户识别对其账户未经授权地访问所使用的方法。注册服务商可以尝试同时使用原始的联系信息和更改后的联系信息发送通知或确认函件，这样，无论此更改是合法提交的还是欺骗性的，也无论该函件的发送是在更改生效之前还是生效之后，都可以增加函件到达正确目的地的可能性。

**针对关键通信提供多种传达方法。**注册服务商可以通过电话、传真、邮政或快递服务向寻求附加保护措施的客户传达重要的通知，而不是完全依赖于电子邮件与客户进行通信。此类服务会让攻击者很难进行未经授权的域名迁移。希望“永久性”续订其极其重要的域名的客户可能会欢迎这种保护措施（并且这种措施在正常的活动中没有任何负面影响）。即使是需要迁移极其重要的域名的客户，在分析风险/益处之后，也会认为处理迁移“交易”所带来的延迟是可以接受的。

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

**鼓励客户参与。**许多大型组织早已习惯于将互联网接入、安全和网络管理外包出去。如今，中小型企业中也开始流行托管服务。托管服务提供商 (MSP) 可以促进客户与提供商之间的合作关系。通过常见问题解答 (FAQ) 或通过网络讲座或播客开展认知培训计划，MSP 可以告诉客户如何有效地利用他们提供的服务。作为上述措施的补充措施，注册服务商可以教育和鼓励注册人：

- 为域帐户指定多个联系点
- 在员工资源管理流程中包含联系信息点管理功能，以确保在废止离职员工的凭据时，与该员工相关联的所有注册域的联系点信息也会随之更改。
- 强制执行密码更改策略。
- 定期验证联系人。
- 主动监控域名注册。
- 为所有的注册联系点分配属于注册域名之外的域的电子邮件地址。（某些注册人可能希望创建多个域注册帐户，以此作为附加的保护措施。）
- 将尝试迁移域名的活动视为安全事件（检查并复查）。
- 对域注册联系人电子邮件帐户和其他业务目的分别使用不同的域。例如，为 example.info 的联系点分配 example.net 的电子邮件地址。
- 创建角色帐户：例如，domainadmincontact@example.com、domainregistrantcontact@example.biz 和 domaintechnicalcontact@example.net。（注意：在使用角色帐户时，强烈建议定期检查此类帐户以确保不会由于组织内部人员、管理或运营方面的变动而中断注册人员对该角色帐户的监控。）
- 为一个角色帐户指定多个通知收件人。使用这种形式的邮件轰炸可实现“地毯式地发送”重要的注册服务商函件，从而增大收到函件和及时处理函件的可能性。

**告知客户。**注册服务商应努力了解他们提供的安全措施，就像了解他们提供的其他竞争性服务一样。例如，如果注册服务商定期将其运作交给独立安全审核机构审核并且通过审核，这种自律可能会引起公众的注意。或者，ICANN 和注册服务商可以联合指定独立安全审核机构并与该审核机构签订制定一套安全措施的合同。注册服务商可以自愿请审核机构对其运作进行审核。通过审核的注册服务商会获得证明其符合安全标准的某种形式的信任标志或公

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

章，从而突出自身的优势。SSL 证书颁发机构也提供类似的计划。<sup>32-33</sup> SSAC 强调信用卡处理在注册服务商中非常普遍，因此，支付卡行业安全审核程序对于商家，数据安全标准要求对于服务提供者，都具有重要的意义。<sup>34</sup>

**先前 SSAC 报告中提出的措施。**许多注册服务商已经实施了 SAC007 “域名劫持报告”中 5.2 节“注册服务商可以采取的域名保护步骤”中推荐的部分或全部措施。现对先前和新近建议的措施归纳如下：

1. 为每个注册域名（而不是每个域注册帐户）使用一个唯一的 EPP authInfo 代码值。有些注册服务商对同一注册人持有的所有域使用同一个 EPP authInfo 代码值。这种做法会导致攻击者只需获取一个代码，客户注册的所有域名便会暴露无遗。
2. 各个注册服务商之间建立统一的域名锁定默认设置。许多注册服务商已自动锁定域名。注册服务商必须提供可以解除域名锁定的充分而直接的方法，以免不恰当地拒绝来自经过验证的域名注册人的合法迁移请求。
3. 研究其他提高注册人记录准确性的方法。考虑更频繁地传达通知或改变通知的形式（例如使用电话作为电子邮件的替补方案），以督促注册人及时更新其信息和检测注册滥用。
4. 从注册人、注册服务商和转销商收集应急联系点信息并提供给适合协助响应紧急恢复域名事件的各方。<sup>35</sup> 制定在无法与应急联系人取得联系的情形下各方一致同意实施的戒备升级流程（应急措施）。
5. 考虑可改善所有注册业务流程中的身份验证和授权的措施。
6. 保护可被用来为欺诈和仿冒以及窃取域名提供方便的注册人信息。默认情况下，注册人身份验证流程中使用的任何信息均应视为机密信息。考虑将此类信息与信用卡或其他金融信息同等对待，采取相同或相似的措施予以保护。
7. 加强对转销商是否遵守记录保留要求的审核。
8. 确保转销商理解注册服务商（和 ICANN）的记录保留要求并促使转销商更好地遵循这些要求。
9. 应以通俗易懂、方便查阅的方式为注册人提供有关注册服务商提供的域锁定和域名保护措施的信息。

---

<sup>32</sup> Thawte Site Seal: <https://www.thawte.com/ssl-digital-certificates/trusted-site-seal/index.html?click=site-seal-tile>

<sup>33</sup> VeriSign Secured Seal®: <http://www.verisign.com/ssl/secured-seal/>

<sup>34</sup> PCI 安全标准委员会: <https://www.pcisecuritystandards.org/>

<sup>35</sup> 另请参阅 SAC 038, Registrar Abuse Contacts: <http://www.icann.org/committees/security/sac038.pdf>

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构（ICANN）已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

## 防止 DNS 配置信息遭到滥用

未经授权地访问域注册帐户的目的之一是控制组织的域名解析服务。攻击者修改目标域名服务器的域名或 IP 地址，使之指向攻击者运作的系统，此系统常常是其之前已经侵入的计算机。在对域名攻击得手之后，攻击者会将该域名的 DNS 服务器和区域文件托管在已被他们控制的计算机上。攻击者的 DNS 服务器会解析该域的名称并将其重定向到恶意或恶搞网站（就像本报告以及 SAC007 中介绍的 Comcast、ICANN、Panix 和 Hush 通信事件中那样）。有些攻击者并不会恶意篡改 DNS 配置信息，而是使用已控制的域注册帐户将其自己的域名服务器添加到原本合法运行的域名服务器列表中。这样可以在 *double flux* 形式的 *fast flux* 攻击中隐藏他们自己的域名服务器<sup>36</sup>，还可防止被逮住。这两种技术都可以延长钓鱼、垃圾邮件、欺诈或犯罪攻击的持续时间。

上文介绍的措施适合希望阻止未经授权地使用客户的域名帐户恶意篡改或悄悄添加 DNS 配置信息的注册服务商。特别是，由注册服务商作为可选服务提供或由注册人执行的下列措施可以为防御 DNS 配置攻击提供重要的保护作用：

- 要求对 DNS 的配置更改进行多因子身份验证。
- 要求使用电子邮件（可能还包括通过电子邮件之外的其他手段）向多个联系人确认更改。（Note:前面介绍的多步验证方法在此处也可能适用。）
- 在执行更改时向多个联系人发送通知。
- 监控 DNS 异常更改或滥用。

此外，注册服务商应当通过常见问题解答、培训和教育来鼓励客户始终监控 DNS 配置活动（更改和添加）。注册服务商还应鼓励客户验证其域内的名称解析到了目标 IP 地址。此外，注册服务商还应督促客户保留所有域的 DNS 配置历史记录，并应帮助客户认识为此信息添加时间戳和数字签名的价值。

---

<sup>36</sup> SAC 025 Fast Flux Hosting and DNS: <http://www.icann.org/committees/security/sac025.pdf>

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构（ICANN）已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

## 调查结论

根据本报告中介绍的事件和相关研究，SSAC 做出下列补充调查结论。

**调查结论 (1)** 注册服务商之间在域名帐户的安全漏洞和防范攻击能力方面存在差异。许多域注册人似乎没有足够的信息来评估注册服务商能在多大程度上帮助其域帐户抵御攻击和防止 DNS 配置遭到恶意篡改。

**调查结论 (2)** 尽管许多注册服务商都提供以普通用户为主要服务对象的域名注册服务，但也有少数注册服务商和“品牌管理”组织为具有广泛影响力、成为众矢之的的域名持有人提供安全服务（通常作为整体品牌权益保护服务的一部分），SSAC 指出“业务专一而又注重安全”的注册服务提供者可谓少之又少，部分原因是客户在选择注册服务商时针对安全措施的评估在客户决策中并未占据重要的位置。

**调查结论 (3)** 注册服务商可以更多地向客户宣传关于他们的安全措施的信息，让客户能够做出知情的决策。自愿将其运作交给独立安全审核机构审核并公开宣传通过此类审核的结果，可让客户根据安全需求、成本和其他附加功能（例如 Web 和 DNS 托管）更好地选择注册服务商。

**调查结论 (4)** 对于帐户登录时使用的身份验证方法，注册服务商（和注册人）过于信任单因子身份验证方法。这种身份验证方法已被各种形式的社会工程攻击、暴力攻击和其他技术一而再、再而三地蒙蔽过关。

**调查结论 (5)** 攻击者在侵入域注册帐户之后便将矛头直指 DNS 配置。由于 DNS 的分布式特性，即使注册服务商已经恢复 DNS 配置信息并力图消除负面影响，被篡改的 DNS 配置信息所带来的影响还会延续一段时间。恶意篡改或不正确的 DNS 信息会在整个互联网的不同位置中持续存在一段时间，此时间等于与被修改的 DNS 资源记录相关联的 TTL 值所代表的全部持续时间。攻击者也许会专门为此修改 TTL。

**调查结论 (6)** 通常，某个用户在注册帐户门户网站通过身份验证或者登录之后，该用户（或仿冒者）便会获得全局权限并可修改联系信息和 DNS 配置信息。以可选服务的形式为客户提供细化的访问控制功能，特别是提供限制每个联系点能够执行的操作类型（更改联系信息和 DNS 配置信息和授权迁移域名）的功能，这样可以降低或减轻域名及其相关联的域名解析服务遭到非法利用或滥用的风险。

**调查结论 (7)** 注册服务提供者更多地依赖未经核实的电子邮件来发送与安全有关的函件（例如，更改通知），而罔顾电子邮件的传递是否有保证以及电子邮件的安全性。攻击者在通过已控制的注册帐户修改域的 DNS 配置之后，常常会通过阻止发送电子邮件来挫败这种通讯方法。允许客户选择备用联系方式或扩展通知服务使之包含某种形式的收到确认，这样可以降低或减轻域名及其相关联的域名解析服务遭到非法利用或滥用的风险。

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

## 建议

*SAC007 针对注册服务商提供了具体的建议；特别是*

**建议 SAC007-(8)：**注册服务商应增强注册人对域名劫持和注册人仿冒和欺诈等威胁的意识，强调注册人需要保持注册信息的准确性。注册服务商还应告知注册人注册服务商锁定功能的可用性和用途并鼓励注册人使用该功能。注册服务商应进一步告知注册人授权机制 (EPP authInfo) 的用途，并应制定建议措施帮助注册人保护他们的域，包括始终监控域名状态，及时、准确地维护联系人信息和身份验证信息。

根据我们对最近事件的分析、相关的研究和我们的调查结论，SSAC 提出以下建议：

**建议 (1)** 我们鼓励注册服务商为希望或需要防止其域名注册服务遭到非法利用或滥用的客户提供更强大的保护措施。本报告中列举的一些措施可作为可选服务单独或捆绑提供给客户。

**建议 (2)** 注册服务商应当扩充他们目前为注册人提供的常见问题解答和教育计划，使之包含安全意识方面的内容。注册服务商应努力让客户能够更方便地访问与他们提供的域注册帐户保护服务有关的信息，让客户在选择注册服务商时可在保护措施方面做出知情的决策。

**建议 (3)** 注册服务商应考虑自愿安排对其运作进行独立安全审核的价值所在，此安全审核可作为其安全尽职调查的一部分。

**建议 (4)** ICANN 和注册服务商应考虑下述问题：根据注册服务商的邀请安排有资质的第三方按照规定的安全标准执行安全审核，是否能够普遍改善注册服务以及是否有益于注册人。ICANN 可参照 SSL 证书颁发机构为符合该机构的安全标准的网站运营商颁发信任标志或加盖公章的方式，通过一项信任安全标志计划，来突出自愿接受并满足此项安全审核基准的注册服务商的优势。

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>.

## 致谢

在 SSAC 研究此问题的过程中，以下成员为撰写和修订本报告付出了宝贵的时间，在此本委员会谨致以诚挚的谢意：

Jaap Akkerhuis

KC Claffy

Steve Crocker

Patrik Fältström

Duncan Hart

Jeremy Hitchcock

Rodney Joffe

Warren Kumari

Danny McPherson

Dave Piscitello

Dan Simon

John Schnizlein

Bruce Tonkin

Rick Wesson

Richard Wilhelm

## 利益声明

以下链接中包含 SSAC 成员的个人简介和利益声明：

<http://www.icann.org/en/committees/security/biographies.htm>。

## 反对意见

委员会中没有成员对发布本报告持反对意见。

本文档译自英文版本，旨在方便更广泛的读者。虽然互联网名称与数字地址分配机构 (ICANN) 已尽力确保译稿的准确性，但英语是 ICANN 的工作语言，本文档的英文原稿是唯一正式、权威的版本。您可以在以下链接中找到英文原稿：  
<<http://www.icann.org/committees/security/sac040.pdf>>。