CN

SAC 028
SSAC 关于假冒注册服务提供商进行仿冒攻击的咨询报告

翻译注释

本文档的原始版本是英文版，可从以下网址获得：http://www.icann.org/committees/security/sac028.pdf。如果翻译文档与原始文档有出入，或者在理解上有出入，请以原始文档为准。

ICANN
安全和稳定
咨询委员会 (SSAC) 的
咨询报告
2008 年 5 月

引言

本咨询报告介绍了以域名注册人为目标的仿冒攻击形式。攻击者会假冒域名注册服务提供商，向注册服务提供商的客户（注册人）发送有关域名相关事项的预期信件。预期信件的示例包括：关于正在处理域名注册期满事宜的通知、产品宣传电子邮件、用于告知注册人帐户管理事宜的通知，或者任何要求或鼓励客户即刻关注的常规信件。不过，此类信件是伪造的。仿冒者会创建一个类似于注册服务提供商站点的伪造网站，引诱客户使用其域管理帐户，使其在不经意间将帐户凭据泄露给仿冒者。仿冒者会使用捕获到的客户凭据来访问客户的域名组合，更改帐户中的域名 DNS 信息，并利用这些域名展开其他攻击。

在本咨询报告中，SSAC 说明了此类攻击的一般形式。我们考虑了各种注册服务提供商在与客户通信的合法电子邮件消息中所使用的信息类型和格式。我们讨论了仿冒者如何操纵这些信息类型和格式来制作伪造的信件，这些信件旨在通过*社会工程手段*[1] 引诱注册服务提供商的客户访问假冒的注册服务提供商网站。攻击者设计假冒网站来欺骗客户泄露域管理帐户名和凭据。我们论述了当前的一些推荐做法，目的是最大程度地降低或防止常见仿冒目标（如金融机构和大型企业）遭受仿冒攻击的可能性。我们就注册服务提供商可以采取的措施提出了建议，这些建议可以降低他们与注册人之间的信件遭受仿冒攻击的可能性，同时还确定了一些方式，供注册人用来检测这种仿冒形式，以免沦为此类攻击的受害者。

[1] 有关社会工程的更多信息，请参见 *Why Phishing Works*，网址为 http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf。

背景：对攻击的分析

仿冒者会利用商家或金融企业发送给客户的多种电子邮件信件形式来展开攻击[2]。注册服务提供商也使用电子邮件进行多种与域名注册相关的通信活动，包括：

- 域名续费通知
- 域名订购确认
- 注册请求确认
- 域信息修改确认
- WHOIS 数据准确性提醒
- 域名期满或取消通知
- 对（新增）服务和功能的宣传和广告

仿冒者会利用注册服务提供商依赖电子邮件信件这一事实来展开攻击。通过在仿冒攻击过程中假冒注册服务提供商，仿冒者能够将注册服务提供商的客户引诱到一个伪造的注册服务提供商客户登录页面，客户在使用这个页面时可能会不经意地将帐户凭据泄露给攻击者。这些凭据使仿冒者能够以未经授权的方式访问域名管理帐户。帐户中包含一些对攻击者来说有价值的资产：

- 客户的域注册信息，这些信息可能会遭到恶意修改（请参见“威胁前景展望”）。
- （潜在地）信用卡或其他在注册服务提供商处存档的支付形式的使用信息，攻击者可以利用这些信息来购买其他域，然后再将这些域用于恶意用途。

仿冒者会从数个源收集信息，以假冒注册服务提供商进行攻击。仿冒者会从注册服务提供商的“真实”网站中复制必要的页面、图像、徽标和文件，以制作一个可信但伪造的注册服务提供商登录页面。这些内容都放在由仿冒者操作的 Web 服务器上，用于假冒注册服务提供商的登录页面。仿冒者还使用从注册服务提供商与客户往来的典型信件中收集到的信息，对其在仿冒电子邮件中包含的消息进行“个人化”。只要成为目标注册服务提供商的注册人，就可以获得信件。仿冒者会使用 WHOIS 信息来进一步个人化仿冒消息；更严重的是，仿冒

[2] 网络钓鱼和欺诈报告的示例可参见 Anti-Phishing Working Group Phishing 文档 (http://www.apwg.org/phishing_archive/phishing_archive.html) 和 MillersMiles.co.uk (http://www.millersmiles.co.uk/archives.php)。

者能够使用 WHOIS 信息来建立收件人列表，这些收件人均为目标注册服务提供商的注册人。

利用从注册服务提供商信件中收集到的信息

在典型信件中，有些注册服务提供商可能会加入由于域名注册而产生的信息。这些信息可能包括客户登录名（身份）以及客户帐号、交易编号或收据编号。有些注册服务提供商会加入供客户使用的联系信息和服务台信息，包括电话号码、电子邮件地址和 URL（超链接）。有些注册服务提供商使用基于 HTML 的电子邮件消息，他们会加入公司徽标、横幅广告和“商标”图形。

攻击者可以利用这些注册服务提供商加入上述信息的这一事实，以这些注册服务提供商的客户为目标撰写仿冒电子邮件消息。例如，仿冒者可以在电子邮件消息中加入客户帐号和交易编号，对消息进行“个人化”，如以下示例所示（该示例是一封假设的纯文本仿冒电子邮件的消息正文）：

```
感谢您的订购
2005 年 10 月 19 日，星期三，上午 5:18:34

尊敬的客户，

感谢您通过 <注册服务提供商> 进行订购。以下是您近期与我们进行交易的详细信息。
请保存此信息，以备将来参考。

客户编号：123456789
登录名：mumbledyfoodle
收据编号：298884-3340
订购总额：$19.99
客服电话：800-555-1234

您必须登录到您的帐户，才能完成此次交易。请访问以下确认链接，网址为
http://www.<注册服务提供商>.tld/login
```

在这个假设的攻击中，电子邮件中的 URL `http://www.registrar.tld/login` 实际上是一个超链接，它将被解析成其他主机的地址或将受害者引导到其他主机，例如，内嵌在电子邮件中 `http://www.registrar.tld/login` 两侧的 HTML 标记可能类似于

```
<a
href="http://stealyourdomainthisway.tld">http://www.registrar.tld/login</a>
```

单击此链接将导致浏览器打开 `stealyourdomainthisway.tld`。在仿冒攻击中，并不是一定要加入客户信息，而且信息也没必要完全准确。不过，即使所加入

的帐号或交易编号不正确，也能增强欺诈性：消息*“看起来”*是合法的，而且有些客户可能会保留交易详细信息并识别出客户编号，而有些客户则不会，该客户群中的成员就可能会毫无疑问地接受任何编号（或身份）。另外，不正确的信息可以使那些可能因某种原因而忽略消息的注册人重新做出回应。假设有一名注册人 John Smith，他对域名 `smith.tld` 非常重视。他收到了一封 WHOIS 准确性提醒通知，其中包含具有相同姓氏的不同个人的联系信息，如以下假设的 WHOIS 准确性提醒通知所示：

```
发件人：whoisreminders@whoisupdate.com
发送时间：2007 年 12 月 12 日，星期三，上午 11:57
收件人：John Smith
主题：WHOIS 数据提醒通知

尊敬的客户，

根据互联网名称与数字地址分配机构的 Whois 数据提醒政策 (WDRP) 03.41 号决议，
我们提醒您及时更新与域名注册相关的公开 WHOIS 联系数据。截止到 2007 年 11 月
15 日，我们的记录包含如下信息：

域名：smith.tld
注册日期：9-Aug-06
到期日期：9-Aug-08
注册人详细联系信息
姓名：Peter Smith
地址：11 Smith Street
地址：（空）
城市：Smithville
州/省：PA
邮政编码：
国家/地区：USA
管理员详细联系信息
姓名：Peter Smith
电子邮件：psmith@iamtherealsmith.tld
地址：11 Smith Street
地址：
城市：Smithville
州/省：PA
邮政编码：
国家/地区：USA
```

```
电话：7305825074307
注册服务提供商名称：<注册服务提供商>
名称服务器详细信息

如果上述任何信息有误，请务必通过以下网址进行更正：
http://correctmywhoisinfo.tld/login[3]。请记住，根据注册协议中条款的规定，
提供错误的 WHOIS 信息可能导致您的域名注册被取消。
```

John 很担心域名被劫持，于是迅速按指示更正问题。他在匆忙中单击了内嵌的链接，访问了仿冒网站，从而将凭据泄露给了仿冒者。

[3] 在此示例中，内嵌在网络钓鱼电子邮件中的 HTML 标记包含一个 IP 地址而不是域名，例如，<a “href=http://206.197.43.103/login/”> http://correctmywhoisinfo.tld/login 。

利用从 WHOIS 服务收集到的信息

在一次具有代表性的假冒注册服务提供商攻击中，将涉及如下事件（按时间顺序排列）：

1. 仿冒者设立伪造的注册服务提供商客户门户网站（登录站点）。
2. 仿冒者撰写看似来自于注册服务提供商的电子邮件信件。
3. 仿冒者将此电子邮件发送到域名的联系人电子邮件地址。此时，他可以选择以下两种攻击方式：特别以此注册人作为目标进行仿冒攻击，或者将此注册人加入目标注册服务提供商的客户列表，以此列表作为目标进行批量仿冒攻击。
4. 某些注册服务提供商的客户沦为欺诈的受害人，访问了伪造的注册服务提供商客户门户网站，从而泄露了登录凭据。
5. 仿冒者收集注册人的帐户凭据，方便日后滥用。

从上述按时间顺序排列的事件来看，很明显仿冒者需要将客户、域名和提供域名的注册服务提供商关联起来，才能尝试假冒注册服务提供商进行攻击。WHOIS 服务提供了域名注册信息，包括注册人的名称和邮政信息、域管理联络人和技术联络人的电子邮件地址，以及提供域名的注册服务提供商。如下所示的是一个具有代表性的 WHOIS 查询结果：

域 ID：D2347548-LROR
域名：ICANN.ORG
创建时间：14-Sep-1998 04:00:00 UTC
上次更新时间：16-Nov-2007 20:24:23 UTC
到期时间：07-Dec-2011 17:04:26 UTC
注册服务提供商：Register.com Inc. (R71-LROR)
状态：DELETE PROHIBITED
状态：RENEW PROHIBITED
状态：TRANSFER PROHIBITED
状态：UPDATE PROHIBITED
注册人 ID：C4128112-RCOM
注册人名称：(ICANN) Internet Corporation for Assigned Names and Numbers
注册人组织：Internet Corporation for Assigned Names and Numbers
注册人所在街道 1：4676 Admiralty Way, Suite 330
注册人所在城市：Marina del Rey
注册人所在州/省：CA
注册人邮政编码：90292

注册人所在国家/地区：US
注册人电话：+1.3108239358
注册人传真：+1.3108238649
注册人电子邮件：icann@icann.org
管理员 ID：C4128112-RCOM
管理员名称：(ICANN) Internet Corporation for Assigned Names and Numbers
管理员组织：Internet Corporation for Assigned Names and Numbers (ICANN)
管理员所在街道 1：4676 Admiralty Way, Suite 330
管理员所在城市：Marina del Rey
管理员所在州/省：CA
管理员邮政编码：90292
管理员所在国家/地区：US
管理员电话：+1.3108239358
管理员传真：+1.3108238649
管理员电子邮件：icann@icann.org
技术人员 ID：C1-RCOM
技术人员名称：Domain Registrar
技术人员组织：Register.Com
技术人员所在街道 1：575 8th Avenue
技术人员所在街道 2：11th Floor
技术人员所在城市：New York
技术人员所在州/省：NY
技术人员邮政编码：10018
技术人员所在国家/地区：US
技术人员电话：+1.9027492701
技术人员传真：+1.9027495429
技术人员电子邮件：domain-registrar@register.com
名称服务器：NS.ICANN.ORG
名称服务器：A.IANA-SERVERS.NET
名称服务器：C.IANA-SERVERS.NET
名称服务器：B.IANA-SERVERS.ORG

在很多情况下，注册服务提供商或第三方 WHOIS 服务会提供有关域名的其他信息，包括：

- 安全状态（站点是否可以通过 SSL 或 HTTP 进行访问）
- 域记录的创建日期和上次修改日期（在某些情况下，可以获得部分或完整的域历史记录）
- 域记录到期日期

- 注册机构状态（注册机构放置在名称上的 EPP[4] 状态代码：clientTransferProhibited、RedemptionPeriod 等）
- 服务器数据，例如：Web 服务器类型（如 Apache 和 Microsoft IIS）、网站状态（如活动状态）、IP 地址、黑名单状态
- DNS 信息（名称服务器的名称和 IP 地址）
- 注册人搜索（例如，此注册人注册的其他域）
- 域名注册人用来优化搜索的 META 关键字
- 广告

攻击者可以使用从 WHOIS 回应收集到的信息，对注册人批量进行仿冒攻击，或者根据预期信件（例如，域名的未决期满信件）有选择地对注册人进行仿冒攻击。某些 WHOIS 信息可以确定域名的电子邮件联系人，从而确定电子邮件的目标收件人以及仿冒者将假冒的域名提供注册服务提供商（电子邮件发件人）。其他信息也可用于增强消息正文的可信度；例如，域记录的创建日期、上次修改日期和到期日期可用来创建伪造的续费通知，安全状态可用来创建与 SSL 认证问题相关的伪造通知，等等。

[4] 可扩展的供应协议 (EPP)，请参见 RFC 3731，
网址为 http:// www.rfc-archive.org/getrfc.php?rfc=3731

威胁前景展望

通过此类仿冒攻击可以劫持域名，但这通常不是攻击者的主要目标。一旦攻击者有权访问注册人帐户，他即可通过注册服务提供商修改 DNS 记录，进而将这些记录指向在其控制之下的名称服务器。这是利用名称服务进行 Fast Flux 攻击等恶意犯罪行为的通常目的[5]；具体而言，攻击者先将地址指向在其控制之下的系统，然后对生存时间 (TTL) 值进行操控，并在他所操作的名称服务器上更改上述地址上域区域数据的 DNS 记录。

除了利用 DNS 进行 Fast Flux 攻击外，攻击者还可以进行其他恶意活动。例如，攻击者可以在他所控制的域区域数据中添加或修改以下记录：

- **MX**，以便指向在其控制之下的邮件主机并使用这些主机发送垃圾邮件。比起可以直接注册的域，攻击者更偏爱使用注册人的域，因为在多数情况下，注册人的域都受到其他邮件系统的信任；也就是说，此类域没有自行发出垃圾邮件的历史或中继垃圾邮件的恶名，也没有被列入过黑名单或另被阻止转发电子邮件。

- **A** 或 **AAAA**，以便指向同样在其控制之下的寄宿欺诈网站的系统（网站往往是最常被修改的，但 FTP 的 IP 地址以及其他寄宿服务的内容也都可以通过此方式进行修改）。然后，攻击者即可将他所选择的任何内容寄宿在假冒网站上；例如，攻击者可能会选择破坏网站的外观，使注册人无法正常使用该网站。

  仿冒者也可能会用错误信息替换网站内容，从而破坏注册人的业务。这种攻击形式的示例包括：公布产品的巨额折扣价、产品召回等。攻击者也可能添加看起来无害的超链接，将点击链接的用户引导到寄宿恶意可下载内容或是用恶意内容替换预期可下载的小程序和可执行文件的网站。

- **A** 或 **AAAA**，以便指向同样在其控制之下的寄宿欺诈内部网站或客户网站的系统。攻击者可能会将目标锁定在具有以下功能的公司：通过身份验证页面提供对敏感信息的 Web 访问权。攻击者通过将 DNS 记录指向在其控制之下的假冒内部网身份验证页面，希望可以欺骗那些未起疑心的员工泄露用

[5] 请参见 SAC022，*Fast Flux 攻击和DNS*，
网址为 http://www.icann.org/committees/security/sac025.pdf

户名和密码，以便日后出售或在攻击该公司时使用。金融机构往往是此类攻击的选择目标，因为客户泄露的帐户信息可能会导致发生欺诈性交易和资金窃取行为。那些提供对敏感信息、专有信息或个人信息的访问权的企业和组织，虽然受到隐私管理法规的保护，但是也会面临遭受此类攻击的风险。

上述内容并不是详尽列表，只是列出了仿冒者近来设法添加或更改的一些具有代表性的 DNS 记录类型。

添加或更改 DNS 记录

与替换 DNS 记录相比，仿冒者似乎更偏爱添加 DNS 记录，因为当注册人的域中有部分或全部名称继续按预期进行解析时，注册人可能很久都不会发现已受到攻击。此外，攻击者希望通过滥用声誉良好的注册人所持有的域名，在反仿冒响应人员和品牌保护人员做出滥用断言时引入不确定性因素。注册服务提供商可能会有所犹豫或拒绝对信任的客户采取措施、坚持法院的判决等等，从而延误了工作来中止以该域名进行的任何相关非法活动。

攻击者也会使用由注册服务提供商提供的域管理工具来实现域的重定向或更改，进而将 DNS 记录指向其他（链接）位置。如果遭到仿冒攻击的客户是利用注册服务提供商来寄宿网站或电子邮件，则攻击者可以上传并修改客户网站上的内容，创建电子邮件帐户（用于发送垃圾邮件），还可以访问、修改或转发该域内现有的电子邮件帐户。

注册服务提供商如何减少仿冒威胁

仿冒者扩大了其攻击范围，不仅包括商业和金融机构，还包括域注册服务供应商。注册服务提供商和分销商必须做出回应确认自己是仿冒的目标。SSAC 建议注册服务提供商（和分销商）在撰写要发送给客户的信件时加以谨慎，并遵循反仿冒的最佳做法。强烈推荐以下几种做法：

1. 在发送给客户的信件中仅包含传达所需消息的必要信息。请勿包含客户帐号、身份和（一般而言）注册信息。这些信息为仿冒者个人化电子邮件创造了机会。

2. 在与客户通信时，避免使用超链接参考。仿冒者通常会伪装链接，将用户从合法页面重定向到欺诈页面。

3. 警告客户不要单击任何信件内的超链接，无论是文本形式还是图像形式。在所发送信件的消息正文中加入以下声明："为免遭仿冒攻击，请在网络浏览器的地址栏中键入以下网址"或"请勿相信电子邮件中的链接。任何情况下都要在浏览器的地址栏中键入网址"。许多客户都会欣赏这种对其安全和隐私表示关心的表达方式，即使与单击地址相比，键入网址会有所不便。

4. 对注册服务提供商也是仿冒攻击目标这一事实提高警觉性。提供（或扩充现有的）常见问答页面，将注意力集中到以下几方面：假冒注册服务提供商仿冒、仿冒攻击造成的威胁、为阻止仿冒所采取的措施，以及客户为检测和避免遭受此类攻击所采取的措施。说明要在电子邮件信件中予以提供的信息类型，并特别明确信件中*"永远不会"*包含的信息类型，这样客户就具备了基础性认识，进而可以评估其所收到的信件是合法的还是可疑的。

5. 为客户提供报告可疑性仿冒攻击的渠道，可以直接提供这样的渠道，或者与某个鼓励提交可疑的欺诈性及诈骗性电子邮件并维护有仿冒电子邮件库的组织进行合作[6]。

6. 考虑针对客户信件实施具有不可否认来源的电子邮件形式，例如电子签名。

[6] APWG 的*报告网络钓鱼*页面网址 http://www.antiphishing.org/report_phishing.html

注册人如何避免成为假冒注册服务提供商的牺牲品

注册人有责任保护其域名投资。就互联网平台服务、操作和商务这几个方面而言，这种责任的重要性不亚于保护身份安全免遭窃取和滥用的责任。消费者安全组织、金融机构和信用卡公司提醒消费者要小心在线诈骗和欺诈，并介绍了如何检测并避免仿冒攻击。此类建议大多都可用于避免假冒注册服务提供商仿冒攻击。下文重申了部分最中肯的建议：

1. 请勿单击所接收电子邮件消息中的超链接。而是在网络浏览器的地址栏中手动键入网页地址。

2. 使用提供反垃圾邮件和反仿冒功能的电子邮件客户端，或安装声誉好的加载项或插件来为电子邮件客户端补充此类功能。

3. 使用可显示与电子邮件地址中所显示文本或图像相关的超链接参考的电子邮件客户端，或了解查看和阅读“源”或纯文本 (ASCII) 电子邮件消息的方法。了解如何阅读 HREF 之类的超链接标记，进而快速检测出链接显示为 `www.example.com` 但实际会将您导向到攻击者域（如

   `<A HREF=“http://iwillscamu.tld”>www.example.com</a>`）

   或 IP 地址（如

   `<A HREF=“http://192.168.2.3”>www.example.com</a>`）的欺诈技术。

4. 不要轻易相信那些要求紧急回应、而唯一的回应方式是访问网站的电子邮件信件。大多数著名的在线公司（包括注册服务提供商）都会提供其他联系客户支持的方法，如电话、电子邮件地址或传真。如果觉得可疑，请使用另一种备选联系方式回应注册服务提供商，最好是找到可以直接访问注册服务提供商的方法。

5. 仔细阅读电子邮件消息正文。通常，错误的语法和标点可以表明电子邮件是伪造的。

6. 请勿仅仅因为电子邮件是个人化的就轻易相信。

7. 在验证网页合法性之前，请勿在任何网络提交表格中泄露个人信息或帐户信息。

8. 通过使用 SSL 确保所访问的任何网络提交表格或登录页面安全可靠。但是，请勿仅仅因为超链接看起来像是安全的页面就轻易相信。验证 SSL 页面相关的数字认证的真实性[7]。

9. 如果想要使用信用卡购买域名服务，请选择要求客户在交易时提交信用卡验证码 (CVV) 的注册服务提供商。CVV 是信用卡公司用来在您购买时验证所持有信用卡的安全措施。

10. 将可疑的仿冒电子邮件报告给注册服务提供商或反仿冒组织，如 APWG、Phish Report Network[8]、PhishTank[9]，或者本地的 CERT[10]。

有关如何避免遭受仿冒者侵害的更多信息，请参阅由反仿冒工作组[11]、PhishTank 和 SpamHaus Project[12] 提供的消费者建议页面。

结论

一般而言，域名已成为非常有价值的商品，曾提供过值得信赖的互动服务和运行状况的域名会成为攻击者的选择目标。假冒注册服务提供商来获取客户凭据并因此获得域名注册访问权构成了严重的仿冒威胁。SSAC 鼓励注册服务提供商和分销商对这种威胁做出回应，确认自己是仿冒的目标，并采取措施防止域名遭到滥用。

SSAC 认识到仿冒的猖獗依赖于欺诈和社会工程。仿冒者尝试破坏注册服务提供商实施的措施。最终，避免遭受欺诈和诈骗侵害的责任还是在于消费者。因此，虽然注册服务提供商可以采取很多措施来遏制仿冒，但是提高客户警觉性并建议客户在回应注册服务提供商信件时加以谨慎是最为重要的。

---

[7] 请参见 SSL.com，Q10068 - FAQ: How can I tell if a web page is secure? 网址为 http://info.ssl.com/Article.aspx?id=10068。

[8] Phish Report Network，网址为 http://www.phishreport.net/

[9] PhishTank：Join the fight against Phishing，网址为 http://www.phishtank.org

[10] 此处包括电子邮件地址或网页。

[11] Consumer Advice: How to Avoid Phishing Scams, 网址为 http://www.antiphishing.org/consumer_recs.html

[12] SpamHaus 的 Project Frequently Asked Pages (FAQ) 索引，网址为 http://www.spamhaus.org/faq/index.lasso