SAC 028
SSAC Advisory on Registrar Impersonation Phishing Attacks

An Advisory from the ICANN
Security and Stability
Advisory Committee
(SSAC)
May 2008

Introduction

This Advisory describes a form of phishing attack that targets domain name registrants. The attacker impersonates a domain name registrar and sends an expected or anticipated correspondence to a registrar's customer (a registrant) regarding a domain name related matter. Examples of expected correspondence include a notice of pending expiration of a domain name registration, a promotional email, a notice informing the registrant of an account management issue, or generally, any correspondence that requires or encourages a customer's immediate attention. The correspondence, however, is bogus. The phisher creates a web site that is deceptively similar to the registrar's site to induce the customer into accessing his domain management account and unwittingly disclose his account credentials to the phisher. The phisher will use the customer's captured credentials to access the customer's domain name portfolio, alter DNS information of domain name(s) in that account and use the domains to abet additional attacks.

In this Advisory, SSAC describes generic forms of this type of attack. We consider types and formats of information included in legitimate email messages that various registrars use when corresponding with customers. We discuss how phishers manipulate these information types and formats to create a bogus correspondence that is designed to *socially engineer*[1] the registrar's customer into visiting an impersonated registrar web site. The attacker designs the impersonated web site to dupe the customer into disclosing domain management account names and credentials. We discuss some of the current recommended practices to minimize or prevent phishing attacks employed by common phishing targets such as financial institutions and large corporations. We recommend measures that registrars can take to make their correspondences with registrants less "phishable" and identify ways for registrants to detect and avoid falling victim to this form of phishing.

[1] See *Why Phishing Works*, http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf, for more information about social engineering.

Background: Anatomy of an attack

Phishers exploit many forms of email correspondence that merchants or financial businesses send to customers[2]. Registrars also use electronic mail for many types of domain name registration-related correspondence, including:

- Domain name renewal notices
- Domain name order confirmations
- Registration request confirmations
- Domain information modification confirmations
- WHOIS data accuracy reminders
- Notices of domain name expiry or cancellation
- Promotions, advertising for (new) services and features

Phishers exploit the fact that registrars rely on email correspondence. By impersonating (spoofing) a registrar in a phishing attack, the phisher is able to lure a registrar's customer to a bogus copy of the registrar's customer login page, where the customer may unwittingly disclose account credentials to the attacker. These credentials provide the phisher with unauthorized access to a domain name management account. The account has several assets of value to the attacker:

- The customer's domain registrations, which can be modified for malicious purposes (see Threat Landscape)
- (Potentially), the use of credit cards or other forms of payment on file at the registrar which could be used to purchase additional domains that can subsequently be used for malicious purposes.

Phishers gather information from several sources to perpetrate a registrar impersonation attack. The phisher copies pages, images, logos, and files necessary to produce a credible albeit bogus copy of the registrar's login page from the registrar's "authentic" web site. These are hosted at a web server operated by the phisher and are used to spoof the registrar's login page. The phisher also uses information gleaned from the registrar's typical correspondences with customers to "personalize" the message he includes in the phish email. Correspondences can be obtained by simply becoming a registrant of a targeted registrar. The phisher uses WHOIS information to further personalize phish messages; more importantly, the phisher is able to use WHOIS information to build a list of recipients who are registrants of a targeted registrar.

Exploiting Information Gathered from Registrar Correspondence

In typical correspondences, some registrars may include information derived from the domain name registration. They may include customer login (identity) and customer account, transaction or receipt numbers. Some registrars include contact and helpdesk information for customers, including telephone numbers, email addresses, and URLs

[2] Examples of phishing and scam reports can be found at the Anti-Phishing Working Group Phishing archive (http://www.apwg.org/phishing_archive/phishing_archive.html) and MillersMiles.co.uk (http://www.millersmiles.co.uk/archives.php).

(hyperlinks). Some registrars who use HTML-based email messages include company logos, banner advertisements, and "branding" graphics.

Attackers can exploit the fact that these registrars include such information when they compose phish email messages targeted at these registrars' customers. For example, a phisher can include customer account and transaction numbers to *personalize* the message, as demonstrated in the following example message body of a hypothetical plain text phish email:

```
THANK YOU FOR YOUR ORDER
Wednesday, October 19, 2005 5:18:34 AM

Dear customer,

Thank you for ordering from <registrar>. Here are the details of your
recent transaction with us. Please save this information for future
reference.

CUSTOMER NUMBER: 123456789
LOGIN NAME: mumbledyfoodle
RECEIPT NUMBER: 298884-3340
ORDER TOTAL: $19.99
CUSTOMER SERVICE: 800-555-1234

You must login to your account to complete this transaction. Please
visit the following confirmation link at
http://www.<registrar>.tld/login
```

In this hypothetical attack, the URL `http://www.registrar.tld/login` is actually a hyperlink in the email that would resolve or direct the victim to a different host, e.g., the HTML tag embedded in the email around `http://www.registrar.tld/login` might look like

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

Clicking on this link would cause a browser to visit `stealyourdomainthisway.tld`. The inclusion of customer information is not absolutely necessary for the phishing attack, nor is it necessary for the information to be entirely accurate. However, the inclusion of even an incorrect account or transaction number enhances the deception: the message *looks* legitimate, and while some customers may retain transaction details and may recognize customer numbers, others do not, and members of the latter group may accept any number (or identity) without question. Alternatively, inaccurate information could evoke a response from a registrant who might otherwise ignore a message. Consider a fictitious registrant, John Smith, who highly values a domain name, `smith.tld`. He receives a WHOIS accuracy reminder containing contact information for a different individual with the same surname, as illustrated in the hypothetical WHOIS accuracy reminder below:

```
From: whoisreminders@whoisupdate.com
Sent: Wednesday, 12 December 2007 11:57 AM
To: John Smith
Subject: WHOIS Data Reminder
```

```
Dear Valued Customer,

In accordance with Internet Corporation of Assigned Names and Numbers
Whois Data Reminder Policy (WDRP) resolution 03.41, we remind to you
keep the public WHOIS contact data associated with your domain name
registration up-to-date. Our records include the following
information as of 15-Nov-07:

Domain Name: smith.tld
Registration Date: 9-Aug-06
Expiration Date: 9-Aug-08
Registrant Contact Details
Name: Peter Smith
Address: 11 Smith Street
Address: (null)
City: Smithville
State/Province: PA
Post code:
Country: USA
Administration Contact Details
Name: Peter Smith
Email: psmith@iamtherealsmith.tld
Address: 11 Smith Street
Address:
City: Smithville
State/Province: PA
Post code:
Country: USA
Phone: 7305825074307
Registrar Name: <registrar>
Name server Details

If any of the information above is inaccurate, you must correct it by
visiting http://correctmywhoisinfo.tld/login[3]. Please remember that
under the terms of your registration agreement, the provision of
false WHOIS information can be grounds for cancellation of your
domain name registration.
```

Fearful of a domain name hijacking, John reacts quickly to correct the problem. In his haste, he clicks on the embedded link, visits the phishing web site, and discloses his credentials to the phisher.

[3] In this example, the HTML tag embedded in the phish email contains an IP address rather than a domain name, i.e., <a “href=http://206.197.43.103/login/”> http://correctmywhoisinfo.tld/login .

Exploiting Information Gathered from WHOIS services

The chronology of events in a representative registrar impersonation attack is as follows:

1. Phisher sets up a bogus registrar customer portal (login site).
2. Phisher composes an email correspondence that appears to be from the registrar.
3. Phisher send this email to the contact email addresses for the domain name (selectively, i.e., targeting this registrant in particular, or as part of a bulk phish attack against a list of customers of a targeted registrar).
4. Some of the registrar's customers fall prey to the deception, visit the bogus registrar customer portal and disclose login credentials
5. Phisher collects the registrant's account credentials for subsequent misuse.

From this chronology of events, it is obvious that phishers need to correlate a customer, a domain name, and the sponsoring registrar of the domain name to attempt a registrar impersonation attack. WHOIS services provide domain name registration information, including the registrant's name and postal information, email addresses of the domain's administrative and technical contacts and the sponsoring registrar. A representative result of a WHOIS query is illustrated below:

```
Domain ID:D2347548-LROR
Domain Name:ICANN.ORG
Created On:14-Sep-1998 04:00:00 UTC
Last Updated On:16-Nov-2007 20:24:23 UTC
Expiration Date:07-Dec-2011 17:04:26 UTC
Sponsoring Registrar:Register.com Inc. (R71-LROR)
Status:DELETE PROHIBITED
Status:RENEW PROHIBITED
Status:TRANSFER PROHIBITED
Status:UPDATE PROHIBITED
Registrant ID:C4128112-RCOM
Registrant Name:(ICANN) Internet Corporation for Assigned Names and Numbers
Registrant Organization: Internet Corporation for Assigned Names and Numbers
Registrant Street1:4676 Admiralty Way, Suite 330
Registrant City:Marina del Rey
Registrant State/Province:CA
Registrant Postal Code:90292
Registrant Country:US
Registrant Phone:+1.3108239358
Registrant FAX:+1.3108238649
Registrant Email:icann@icann.org
Admin ID:C4128112-RCOM
Admin Name:(ICANN) Internet Corporation for Assigned Names and Numbers
Admin Organization:Internet Corporation for Assigned Names and Numbers (ICANN)
Admin Street1:4676 Admiralty Way, Suite 330
Admin City:Marina del Rey
Admin State/Province:CA
Admin Postal Code:90292
Admin Country:US
Admin Phone:+1.3108239358
Admin FAX:+1.3108238649
Admin Email:icann@icann.org
Tech ID:C1-RCOM
Tech Name:Domain Registrar
Tech Organization:Register.Com
Tech Street1:575 8th Avenue
Tech Street2:11th Floor
Tech City:New York
Tech State/Province:NY
Tech Postal Code:10018
```

```
Tech Country:US
Tech Phone:+1.9027492701
Tech FAX:+1.9027495429
Tech Email:domain-registrar@register.com
Name Server:NS.ICANN.ORG
Name Server:A.IANA-SERVERS.NET
Name Server:C.IANA-SERVERS.NET
Name Server:B.IANA-SERVERS.ORG
```

In many cases, a registrar or third party WHOIS service provides additional information about the domain, including:

- Security status (whether the site is SSL or HTTP accessible)
- Dates the domain record was created and last modified (in some cases, a partial or complete domain history can be obtained)
- Domain record expiration date
- Registry status (the EPP[4] status code the registry has placed on the name: clientTransferProhibited, RedemptionPeriod, etc.)
- Server data, e.g., web server type (e.g., Apache, Microsoft IIS), web site status (e.g., active), IP address, blacklist status
- DNS information (names and IP addresses of name servers)
- Registrant search (e.g., other domains registered by this registrant)
- META keywords the domain name registrant uses to refine searches
- Advertising

Attackers can use information gleaned from WHOIS responses to phish registrants in bulk or to selectively phish registrants based on an anticipated correspondence, e.g. pending domain name expiration. Certain WHOIS information identifies email contacts for the domain name and hence the target recipients for electronic mail as well as the sponsoring registrar that the phisher will impersonate (the email sender). Other information may be used to enhance the credibility of the message body; for example, domain record creation, last modified, and expiration dates can be used to create a bogus renewal notification, security status could be used to create a bogus notification regarding a concern with an SSL certificate, etc.

[4] Extensible Provisioning Protocol (EPP), see RFC 3731. http:// www.rfc-archive.org/getrfc.php?rfc=3731

The Threat landscape

Domain name hijacking via phishing attacks of this kind is possible but not generally the primary objective. Once the attacker has access to the registrant's account, he can modify DNS records via the registrar so that they point to name servers under his control. This is a common purpose for criminal and malicious activities that exploit name service in fast flux attacks[5]; specifically, with address pointers to systems under his control, the attacker can then manipulate time to live values (TTLs) and alter DNS records of the domain zone data on the name servers he operates at those addresses.

The attacker can do more than exploit DNS for fast flux attacks. For example, the attacker can add or modify the following records in the domain zone data he controls:

- **MX**, to point to mail hosts under his control and use these to send spam. Using the registrant's domain is preferable over domain the attacker could register directly because in many cases, the registrant's domain is "trusted" by other mail systems; i.e., it has no history of originating or reputation for relaying spam and is not blacklisted or otherwise blocked from forwarding email.

- **A** or **AAAA**, to point to systems that host spoofed web sites also under his control (web would be the most popular, but IP addresses for FTP and other content hosting services could be modified in this manner as well). The attacker can then host whatever content he chooses at the phony site; for example, the attacker might choose to deface the web site and embarrass the registrant.

  Phishers may also substitute incorrect information on the site to disrupt the registrant's business. Examples of this form of attack include announcements of deep discounts on the prices of products, product recalls, etc. The attacker can also include innocuous-appearing hyperlinks that direct recipients to sites that host to malicious, downloadable content or that substitute malicious content for intended downloadable applets and executables.

- **A** or **AAAA**, to point to systems that host spoofed internal or customer web sites also under the attacker's control. The attacker can target a company that provides web access to sensitive information via an authentication page. By pointing DNS records to a phony intranet authentication page under his control, the attacker expects to dupe unsuspecting employees into disclosing usernames and passwords, which he will sell or use in subsequent, "speared" attacks against that company. Financial institutions would be choice targets for such attacks, as customers would disclose account information that could result in fraudulent transactions and theft of funds. However, businesses and organizations that provide access to sensitive, proprietary, or personal information that is protected by privacy regulations are also at risk to such attacks.

This list is not exhaustive but merely representative of the types of DNS records phishers currently seek to add or alter.

[5] See SAC022, *Fast Flux Attacks and DNS*, http://www.icann.org/committees/security/sac025.pdf

Adding or Altering DNS records

Phishers appear to prefer adding over replacing DNS records because the registrant may remain unaware of the attacks longer if some or all of the names in his domain continue to resolve as expected. Further, by misusing a domain name that is held by a registrant in good standing, the attacker hopes to introduce uncertainty when claims of misuse are made by anti-phishing responders and brand protectors. Registrars may hesitate or refuse to take action against a trusted customer, insist on a court order, etc., which may delay efforts to suspend any illegal activities conducted in association with that domain name.

The attacker may also use domain administration tools provided by the registrar to enable redirection or alter a domain so that DNS records point to another (link) location. If the phished customer uses the registrar to host web or email, the attacker can upload and modify content on the customer's web site, create email accounts (for spam), or access, modify, or forward existing email accounts in that domain.

How registrars can reduce phishing threats

Phishers have broadened their reach beyond merchant and financial institutions and into domain registration service providers. Registrars and resellers must acknowledge that they are phishing targets in response. SSAC recommends that registrars (and resellers) exercise care and follow antiphishing best practices when composing correspondence to customers. The following practices are highly recommended:

1. Only include information necessary to convey the desired message in customer correspondence. Do not include customer account numbers, identities, and (generally) registration information. These create opportunities for phishers to personalize email.

2. Avoid using hyperlink references in correspondence with customers. Phishers commonly disguise links to redirect users from a legitimate page to a spoofed one.

3. Warn customers against clicking on hyperlinks included in any correspondence, in text or image fashion. Include statements in the message bodies of correspondence you send such as, "To protect against phishing, please type the following web address into the address bar of your web browser" or "Do not trust links in email. Always type a web address into your browser's address bar". Many customers will appreciate the expression of concern for their security and privacy, even if inconvenienced by having to type rather than click an address.

4. Raise awareness that registrars are targets for phishing attacks. Provide (or expand existing) FAQ pages to call attention to registrar impersonation phishing, the threats these phishing attacks pose, measures you are taking to deter phishing and measures your customers can take to detect and avoid falling victim to such attacks. Explain the type of information you will include in email correspondence and in particular, identify the types of information that you will *never* include in correspondence so that customers have a basis for assessing whether correspondence they receive is legitimate or suspicious.

5. Provide a means for a customer to report suspected phishing attacks, either directly, or in cooperation with an organization that encourages submission of suspected scam and fraud emails and maintains a repository of phishing emails[6].

6. Consider implementing a form of email non-repudiation of origin for customer correspondence, such as a digital signature.

[6] The APWG *Report Phishing* page at http://www.antiphishing.org/report_phishing.html

How registrants can avoid falling victim to registrar impersonation

Registrants have a responsibility to protect their investments in domain names. This responsibility is no less important in the contexts of Internet presence, operation, and commerce than the responsibility to protect one's identity from theft and misuse. Consumer safety organizations, financial institutions and credit card companies alert consumers to online fraud and scams and explain how to detect and avoid phishing attacks. Much of this advice is applicable to avoiding registrar impersonation phishing attacks. Some of the most relevant advice is reproduced here:

1. Do not click on hyperlinks included in email messages you receive. Instead, manually type the address of the web page in the address bar of your web browser.

2. Use an email client that offers anti-spam and antiphishing features, or install a reputable add-on or plug-in that complements your email client with such features.

3. Use an email client that is able to reveal the hyperlink reference associated with displayed text or images included in an email address, or learn how to view and read the "source" or plain text (ASCII) email message. Learn how to read hyperlink tags such as HREF so you can quickly detect deception techniques that display a link as `www.example.com` but in reality directs you to an attackers domain, i.e.,

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

   or IP address, i.e.,

   ```
   <A HREF="http://192.168.2.3">www.example.com</a>.
   ```

4. Be suspicious of email correspondence that claims an urgent response is required when the only means of responding is by visiting a web site. Most reputable online businesses, registrars included, will include other means of contacting customer support, such as telephone, email address, or fax. When in doubt, respond to your registrar using an alternative means of contact, in particular, one that you find by visiting your registrar directly.

5. Read the email message body carefully. Poor grammar and punctuation are often indicators that the email is bogus.

6. Do not trust an email simply because it is personalized.

7. Do not divulge personal or account information in any web submission form until you verify the page is legitimate.

8. Make certain any web submissions form or login page you visit is secured using SSL. However, do not trust a hyperlink simply because it appears to be a secure page. Verify the authenticity of the digital certificate associated with SSL pages[7].

9. If you intend to purchase domain name services using a credit card, choose a registrar that requires its customers to submit the Card Verification Value Code (CVV) at the time of a transaction. The CVV is a security measure credit card companies use to verify that you possess the card when you make a purchase.

10. Report suspected phishing emails to your registrar or antiphishing organizations such as the APWG, the Phish Report Network[8], PhishTank[9],or your local CERT[10].

For more information on how to avoid falling victim to phishers, read the consumer advice pages provided by the Anti-Phishing Working Group[11], PhishTank, and the SpamHaus Project[12].

Conclusions

Domain names have become highly valued commodities in general, and domain names that have a history of reputable presence and trustworthy operation are choice targets for attackers. Impersonating a registrar to obtain a customer's credentials and thus gain access to domain name registrations is a serious phishing threat. SSAC encourages registrars and resellers to acknowledge that they are phishing targets in response to this threat, and to take measures to prevent abuse.

SSAC recognizes that phishing thrives on deception and social engineering. Phishers will attempt to subvert measures registrars implement. Ultimately, the responsibility to avoid falling victim to scams and fraud lies on the consumer. Thus, while many measures to deter phishing are available to registrars, raising customer awareness and advising customers to exercise care when responding to registrar correspondence is the most important.

[7] See SSL.com, Q10068 - FAQ: How can I tell if a web page is secure? http://info.ssl.com/Article.aspx?id=10068.
[8] Phish Report Network, http://www.phishreport.net/
[9] PhishTank: Join the fight against Phishing, http://www.phishtank.org
[10] Include email addresses or web pages here.
[11] Consumer Advice: How to Avoid Phishing Scams, http://www.antiphishing.org/consumer_recs.html
[12] The SpamHaus Project Frequently Asked Pages (FAQ) Index, http://www.spamhaus.org/faq/index.lasso