Making Waves in the Phisher's Safest Harbor: Exposing the Dark Side of Subdomain Registries

An APWG Industry Advisory

APWG

Committed to Wiping Out Internet Scams and Fraud

November 2008

Correspondent Authors Contact Data:
Dave Piscitello, ICANN: dave.piscitello@ICANN.org
Rod Rasmussen, Internet Identity: rod.rasmussen@InternetIdentity.com

Disclaimer: PLEASE NOTE: The APWG and its cooperating investigators, researchers, and service providers have provided this message as a public service, based upon aggregated professional experience and personal opinion. These recommendations are not a complete list of steps that may be taken to avoid harm from phishing. We offer no warranty as to the completeness, accuracy, or pertinence of these recommendations with respect to any particular registrar's operation, or with respect to any particular form of criminal attack. Please see the APWG website — http://www.apwg.org— for more information.

Principal Investigators:
Dave Piscitello, ICANN
Rod Rasmussen, Internet Identity

Contributing Researcher:
Greg Aaron, Afilias

Summary

Phishers always look for the effective ways to distribute phish email, lure victims to scam web sites, and shield their online scams from discovery and takedown. Phishers make considerable efforts to maintain these shields, and have repeatedly adjusted their attack methods in response to each improvement in antiphishing measures. Domain names have played an increasingly important role in phishing attacks for some time, and they remain a tactical area of great interest to phishers. This advisory discusses how phishers now use what we call *subdomain registries* to provide safe harbors for malicious and criminal activities. The advisory also discusses measures individuals and organizations can consider if they opt to make these harbors less attractive and effective to phishers.

What is a subdomain registry?

Many online businesses provide Internet users with *hosting accounts*. These businesses operate server farms and provide customers with opportunities to host web services, file transfer (ftp), mail or other services for free or for fee. Several business models exist for such operators.

Some providers offer free domain names, free DNS service, and free website hosting in return for the opportunity to post advertising on the customers' web sites. This model accommodates customers who want the provider to host the web site as well as situations where the customer chooses to host a web site on a system that is dynamically assigned an IP address.

Hosting providers also offer free email accounts as well; in this case, advertising is appended to each message the customer sends. Some providers offer web or blog hosting without fee or advertising as a community service and allow users to create vanity domain names.

Other hosting providers are for fee. They accept credit card payments for hosting, allow vanity domain names and DNS service, and impose no advertising commitments on customers. In some cases, vanity domains are offered as part of an enticement package by for fee hosting providers.

Certain of these businesses allow customers to register a subdomain from one of their own registered domains as part of the service package. Simply put, these businesses allow customers to choose a "name" from their own (parent) domain. The general structure for names of this kind is:

<customer_term>.<service_provider_domain_name>.<TLD>[1]

[1] Note: <TLD> represents any ICANN Top Level Domain or registry (e.g. COM, NET, ORG, INFO). <TLD> can also be a *country code Top Level Domain (ccTLD)*, e.g., RU (Russia), FR (France), CO.UK (United Kingdom).

To provide an example, we created a free web hosting account at Free Servers (no longer active). We registered the name

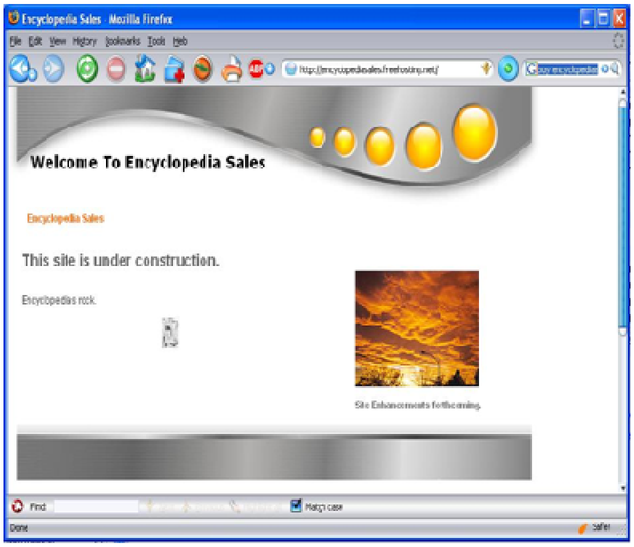
encyclopediasales

as a subdomain of

free-hosting.net,

which is one of the domain choices this provider offers. We created a simple home page for our site, which is now hosted at

http://encyclopediasales.free-hosting.net


Encyclopedia Sales - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Find
Match case
Done

Welcome To Encyclopedia Sales

Encyclopedia Sales

This site is under construction.

Encyclopedias rock.

Site Enhancements forthcoming.

Many businesses administer the domain name service (DNS) customers. Certain businesses allow customers to choose names from domains the business registers. In our example, a business has registered the domain name free-hosting.net and allows customers to "register" names within free-hosting.net. This business manages names like encyclopediasales similar to the way the ICANN Top Level Domain registry COM manages the name APWG or the registry ORG manages the name ICANN.

Because of this similarity, we refer to these businesses as operators of *subdomain registries*. Hosting service companies provide subdomain registrations to serve thousands of customers through a variety of free or for fee business models. The success and popularity of these services illustrate that they satisfy a consumer need.

Why are subdomain registries appealing to phishers?

The services subdomain registries are appealing to phishers for several reasons.

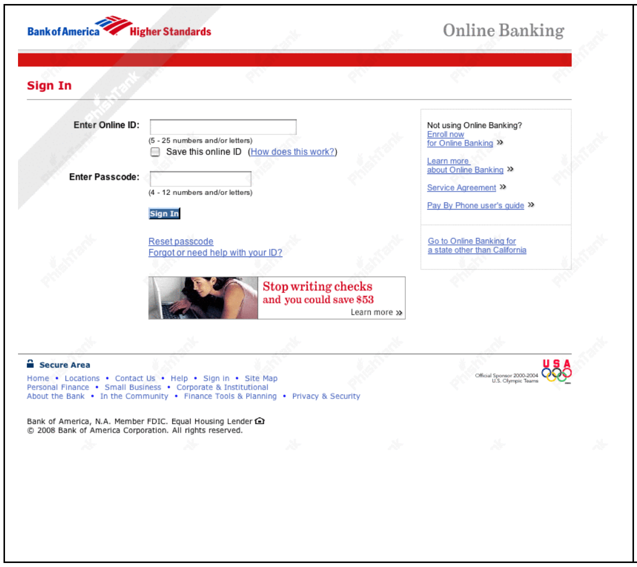
1. Many hosting accounts are free, easy to set up, and simple to remotely administer. In some cases, a subdomain registration only requires a first name and email address for registration.
2. With a small investment of time, phishers can find hosting services where registration is virtually anonymous. Within minutes, a phisher can upload a scam site immediately upon completion of a registration.
3. Subdomain registries do not collect complete and accurate contact information. This exacerbates the already challenging process of deleting or "taking down" a phishing subdomain.

4. Many subdomain registration services have no obvious or formal dispute resolution mechanism.
5. Hosting service providers who fear reputational or other harm to their businesses may be reluctant to suspend a customer account without further investigation, subpoena, or court order.

Subdomain registries accommodate diverse IP addressing models. Some subdomain registries support dynamic IP allocation services or allow customers to redirect their domain names to an IP address the customer chooses. These practices accommodate Internet users who connect through ISPs that assign dynamic addresses. They also allow phishers to host scam web sites on compromised systems. The phishers can also proxy traffic from unwitting Internet users to scam web sites operating from a hosting account via bots operating on compromised systems connected to the same broadband access networks.

Subdomain registries pose serious problems for brand infringement monitoring. Many companies monitor brand abuse directly or through outsourcing companies. These companies scan domains registered through ICANN accredited registrars for abuse and infringement. Subdomain registries add thousands of zones to this monitoring effort, and most of their zones are not readily accessible.

The web sites phishers operate from hosting accounts have an obvious and decidedly different purpose than our Encyclopedia Sales site, as these subdomain phishing examples found at PhishTank.com painfully illustrate:



Sign In

Enter Online ID:
(5 - 25 numbers and/or letters)
□ Save this online ID (How does this work?)
Enter Passcode:
(4 - 12 numbers and/or letters)
Sign In

Reset passcode
Forgot or need help with your ID?

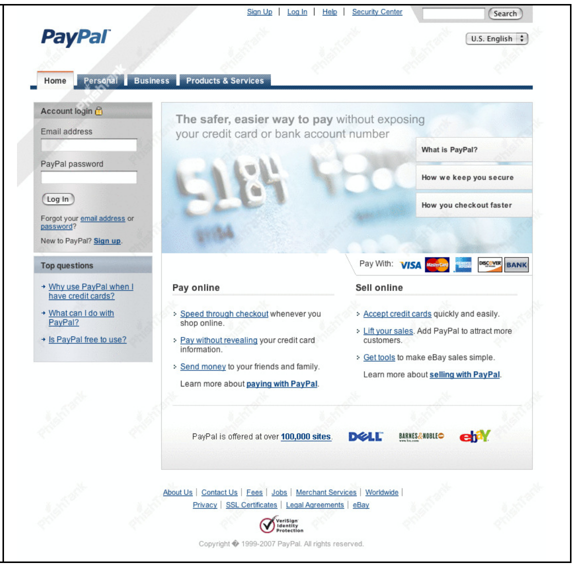
Stop writing checks and you could save $53
Learn more »

Not using Online Banking?
Enroll now for Online Banking »
Learn more about Online Banking »
Service Agreement »
Pay By Phone user's guide »
Go to Online Banking for a state other than California

Secure Area
Home • Locations • Contact Us • Help • Sign in • Site Map
Personal Finance • Small Business • Corporate & Institutional
About the Bank • In the Community • Finance Tools & Planning • Privacy & Security

Official Sponsor 2000-2004 U.S. Olympic Teams
USA

Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2008 Bank of America Corporation. All rights reserved.



Account login
Email address
PayPal password
Log In
Forgot your email address or password?
New to PayPal? Sign up.

Top questions
- Why use PayPal when I have credit cards?
- What can I do with PayPal?
- Is PayPal free to use?

The safer, easier way to pay without exposing your credit card or bank account number

What is PayPal?
How we keep you secure
How you checkout faster

Pay With: VISA MasterCard DISCOVER BANK

Pay online
- Speed through checkout whenever you shop online.
- Pay without revealing your credit card information.
- Send money to your friends and family.

Learn more about paying with PayPal.

Sell online
- Accept credit cards quickly and easily.
- Lift your sales. Add PayPal to attract more customers.
- Get tools to make eBay sales simple.

Learn more about selling with PayPal.

PayPal is offered at over 100,000 sites. DELL BARNES&NOBLE ebY

About Us | Contact Us | Fees | Jobs | Merchant Services | Worldwide |
Privacy | SSL Certificates | Legal Agreements | eBay

VeriSign Identity Protection

Copyright � 1999-2007 PayPal. All rights reserved.

How serious is the subdomain registry problem?

Subdomain registry services offer phishers an attractive, "safe harbor" alternative to registering domains in top level domain registries. The APWG's *Global Phishing Survey: Domain Name Use and Trends in 2007*[1], identified 448 unique second-level domains that offered hosting and subdomain registrations.

Among these, the APWG were able to positively identify 11,443 subdomains hosting sites for phishing. The report's authors believe this figure is conservative, writing that "there are likely more within the data set, as it is often difficult to separate them out from other kinds of domains that have hacked hosts or were registered independently by phishers and set up with special subdomains."

Given this conservative caveat, one might expect that the impact from these domains might not have affected the results of the study. However, the data set of more than 151 million URLs used for this study positively identified 51,989 unique domains as domains used in phishing attacks. Add the 11,443 subdomains to this figure and the result is quite troubling: *subdomain registrations accounted for at least 18% of all domains used in phishing attacks*.

Even more troubling is the dramatic increase in the number of domain names now used by subdomain registries in which APWG and other antiphishing organizations have positively identified phishing domains. By mid-2008, at least one phish site has been associated with a subdomain registered in over 1800 domains. This figure represents a fourfold increase in the number of subdomain registries used by phishers. Subdomain registries are providing safe harbors for phishers and in abundant quantities over the 2007 figure.

What can subdomain registries do to reduce this threat?

Antiphishing organizations need cooperation from subdomain registries to fight this form of phishing attack. We encourage these registries to consider policies and practices that are implemented by many top-level domains today:

1. *Require customers to read and agree to a Uniform Terms of Service agreement (UTS) that prohibits use of subdomains for malicious or illegal activities*. Indicate in the UTS that violation of this term is grounds for an immediate suspension of an account and deletion of the subdomain from the DNS.

[1] Global Phishing Survey: Domain Name Use and Trends in 2007: http://www.apwg.com/reports/APWG_GlobalPhishingSurvey2007.pdf

2. *Collect and maintain accurate contact information*. Individuals who create accounts for consumer, home and small business, and other self-beneficial needs will share contact information with registries if they see a benefit from the request: phishers either can't or won't. This information need not be published or made publicly accessible but it is essential to investigating phishing attacks and helps ensure that accounts are not suspended erroneously.

3. *Provide an abuse handling process for subdomains where users and antiphishing agents can identify accounts that violate the UTS, web pages that host scam or illegal content, etc.* Published abuse contact information prominently on your registration pages.

4. *Monitor the zone file activity for all domains used to register subdomains to detect activities that violate the UTS.*

5. *Implement an accelerated suspension plan.* Develop trust and working relationships with antiphishing agents to reduce the time required to confirm a positively identified phish site and rapidly take it down.

6. *Implement an appeal or dispute resolution process to provide customers a means to appeal and have service restored in the hopefully rare circumstances where a subdomain was erroneously suspended.* (A well-conceived suspension plan, executed with competent trusted parties should assure that the frequency of such incidents is very rare).

The APWG is working with ICANN accredited domain name registrars to develop a set of registrar best practices. Subdomain registries are encouraged to read and apply relevant practices from this report. Subdomain registries may also want to consider working cooperatively with brand owners to reduce Intellectual Property, trademark, and copyright infringement. Some additional measures to consider include:

a) Obtain a list of commonly phished brands and prohibit customers from creating names that infringe on brand, IP or copyrights.

b) Create an access policy for zone files used to register third level labels to allow law enforcement, brand protection companies, and other trusted parties to monitor for abuse.

c) Use CAPTCHA or similar methods to defeat registration and DNS configuration automation.

d) Implement safeguards to defeat DNS abuse. Some measures to consider include limiting the number and frequency of DNS configuration changes and prohibiting DNS configurations that make use of IP addresses from multiple Autonomous System Numbers (ASNs). Dynamic DNS providers should also consider restricting the number of IP addresses that can be used.

Subdomain registries have no choice but to act

In the brick and mortar world, we learn about criminal acts and where they occur from local news reports and word of mouth. We learn where pickpockets routinely separate victims from wallets and the IDs and credit cards they contain, where scheduled controlled substances are made available "under the counter" without a prescription by parties without license, and where illegal materials – from child pornography to copyright protected software and content – can be purchased in plain brown paper wrapping. We steer clear of such neighborhoods and warn our friends and family to do so as well.

An analog exists in the world where we have a virtual presence: steer clear of domains with a history of malicious activities. Consumers and businesses adopt this boycott mentality when they learn about phishing neighborhoods. In effect consumers and businesses change, "If you can't run a respectable establishment we won't visit it" to "if you can't run a respectable hosting service we won't visit **any** of your sites."

Host boycotting is practiced today in several forms, on URLs and individual domains; for example, options in Internet Explorer, Firefox, and Safari allow Internet users to add URL block lists directly to web browsers. Advertisement and content blocking lists such as IE-SPYAD and AGNIS simplify this task for users. "Microsoft shops" can automate the inclusion and install such lists on all machines in their organization by incorporating them in an Active Directory global security policy. Business, schools and universities that make use of HTTP filtering available on web proxies, Internet firewalls, and Unified Threat Management devices can exclude URLs, domains and IP addresses they suspect might harbor phish sites. Many of these security systems offer subscription services that constantly update block lists.

Subdomain registry operators must consider of the cause and blanket effect of URL block listing by security systems. Block listings are triggered when domains appear in spam and phishing email. Certain block listing services strip all information other than the "parent" domain name when they add a name to a block list; for example, services will strip subordinate labels, directories and file names and will block the second level label - <service_provider_domain_name> -in <TLD>. By the very nature of its operation, hosting providers who register subdomains are more like generic or country-specific top level domain registry than ICANN accredited registrars or a domain resellers. A negative reputation based on one or a handful of labels can severely impact an entire service.

One bad actor exploiting your subdomain registration service could lead to automated blocking of your entire domain across a huge swath of the Internet. Indeed, entire domains used by subdomain registries are block listed today. Of the 1800 subdomain registries we identified in 2007, 232 domains are registered in COM. Of these, 27 domains or 12% are block listed by at least one major block list service. If the percent of block listed domains in COM is representative for all TLDs, subdomain registries are already in the cross hairs of antiphishing organizations.

Subdomain registries should take note that frustration with phishing among large enterprise IT staff has passed the breaking point. In certain enterprises, a zero tolerance approach is adopted, and IT will block entire top-level domains based on one or more "phishing prevalence" studies or metrics. The analog here is slightly different from a boycott: "your harbor is not safe, and IT won't allow any of my ships to dock there." Many ISPs operate antiphishing and antispam gateways today, so they are also in a position to enforce as restrictive a blocked site policy as they deem appropriate to protect their customers – and these ISPs may be rewarded with stronger customer retention and growth in market share by acting in this manner.

Avoid the blockade and make waves now

None of these scenarios have positive outcomes for hosting service providers. They tarnish brand, inhibit visitors, provide less exposure for affiliate advertisers, and diminish the appeal of their services to legitimate customers. All that any individual or organization requires in the aforementioned scenarios is a list of subdomain registries that have had one or more positively identified incidents of hosted phishing sites. Such a list is easily composed from available antiphishing feeds manually today. If the trend continues unabated, security companies that compose block lists for subscription antiphishing services could adopt a zero tolerance practice with regard to subdomain registries as well as top-level domains. Subdomain registries should consider the risk of failing to take measures to stem phishing attacks from subdomains before more aggressive processes are implemented.

References:

"Anti-Phishing Best Practices Recommendations for Registrars"
http://www.apwg.com/reports/APWG_RegistrarBestPractices.pdf

"Global Phishing Survey: Domain Name Use and Trends in 1H2008"
http://www.apwg.com/reports/APWG_GlobalPhishingSurvey2007.pdf

IE-SPYAD Restricted Sites List
http://www.spywarewarrior.com/uiuc/resource.htm

AGNIS: AtGuard/NIS/NPF Ad Block List
http://www.spywarewarrior.com/uiuc/resource.htm#AGNIS

Internet Explorer Maintenance Extension Tools and Settings
http://www.spywarewarrior.com/uiuc/resource.htm#AGNIS

PhishTank
http://phishtank.org