Abusive Domain Registrations: ICANN Policy Development Efforts (or Lack Thereof?)

By Mike Rodenbaugh

ICANN, the Internet Corporation for Assigned Names and Numbers, if even recognized, is an enigma to most people. It is a not-for-profit California corporation tasked by the US Department of Commerce to manage the global domain name system (DNS) and IP addressing functions that are fundamental to the operation of the Internet. ICANN has managed these functions for more than 10 years, a period of explosive growth that has seen the DNS expand to more than 174 million names. This total includes 27 percent growth from the end of 2006 to the end of 2007, and 26 percent growth from Q3 2007 to Q3 2008.[1]

This article addresses the current growing problem of abusive domain name registrations, including those registered for cybersquatting, phishing, and malware distribution. This problem will undoubtedly grow with the advent of International Domain Names in alternative scripts, and new top-level domains (TLDs) coming in 2010 and beyond. Yet ICANN has done little to develop policy to deal with these issues. Current status of ICANN efforts, and further potential policy development options are presented in this article.

Mike Rodenbaugh represents clients in all matters relating to domain names, trademarks, copyrights, and other forms of intellectual property and in e-commerce, IP licensing and marketing transactions, and dispute resolution efforts. Mr. Rodenbaugh started his own law and consulting firm in 2007, after more than seven years co-managing trademark and domain name inventory and strategy for Yahoo! Inc., and handling hundreds of different transactions and dispute resolutions for Yahoo! His team managed all matters of protection and infringement of Yahoo!'s trademarks and domain names worldwide and advised on all legal and policy issues involving brand marketing, trademarks, domain names, and rights of publicity. Mr. Rodenbaugh is active in the Anti-Phishing Working Group, International Trademark Association, and ICANN. With respect to ICANN, Mr. Rodenbaugh was elected in 2006 (and re-elected in 2008) to represent the Business Constituency as one of its three Officers and as one of its three Councilors to the Generic Names Supporting Organization (GNSO). The GNSO develops policy relating to generic top-level domain space, such as .com, .net, .org, .biz, .info, .travel, .jobs and many new gTLDs coming in 2010 and beyond. Mr. Rodenbaugh thanks his colleague, Erin Dennis Vivion, for her valuable research and drafting assistance in writing this article.

Cybersquatting: Domain Tasting & Kiting

Most trademark lawyers are probably aware that ICANN is involved with managing the DNS and developed the Uniform Dispute Resolution Policy (UDRP) arbitration remedy for trademark cybersquatting. This remedy was intended to deter cybersquatting by providing a fast-track arbitration process so that trademark owners would not have to resort to court action to recover squatted names. Enacted in 2000, a record number of more than 3,000 UDRP complaints were filed in 2007, with some 25 percent settled before a decision, and 85 percent of decisions in favor of the complainant.[2]

Unfortunately, because the cost of filing a UDRP action is anywhere from 200 to 2,000 times greater than the cost of registering a .com domain name, literally millions of clearly infringing domains are currently registered to cybersquatters. A 2008 brand-jacking report by MarkMonitor found 420,000 cybersquatted domains with respect to just 30 brands.[3] As that statistic indicates, many well-known online brands try to prioritize efforts against more than 10,000 infringing domain registrations at any given time. Increasingly, squatters are registering country code domains, as most ccTLD registries no longer impose meaningful restrictions on registrations, registration costs are dropping, and overall Web traffic continues to grow rapidly in most countries.

Abuse of the DNS has become a fundamental tool of trademark infringers, who register domains that are misspellings of trademarks, trademarks with omitted characters, and trademarks combined with other words, numbers, or symbols. The infringers then hijack direct navigation traffic intended for the trademark owner and often try to drive further traffic to the domains via spam, search engines, and other means. Typically, they monetize traffic by advertising to it. The trademark owner and its competitors often pay these advertising costs indirectly.[4] The registrant and their advertising distributor share ad revenue on every click or pop-up, while a domain registry, registrar, and ICANN share revenue from every registration.

This activity has been taken to the extreme over the past several years, with the rise of "domain tasting" and

"domain kiting" as profitable business practices. Tasters take advantage of the five-day "Add Grace Period" required in most of ICANN's gTLD registry contracts, including Verisign's contracts to operate .com and .net. They have developed software to select thousands or even millions of names at a time, register them all, monetize them and track traffic for almost five days, and then drop almost all of the domains for a full credit of the registration fee. They keep only those few domains projected to earn more than their registration fee via pay-per-click (PPC) traffic over 365 days.[5]

The cybersquatting problem is likely to continue to grow unless and until ICANN implements a policy that actually deters this insidious practice.

Even less scrupulous yet still profitable tasters have formed many different companies to "kite" domains by re-registering their dropped domains for another five days and continuing the cycle. Thus avoiding registration costs entirely, yet maintaining continuous control of the kited domain names. Several famous brand owners have been aggressive in litigating against these types of cybersquatters. Often the filed complaints in these actions list thousands of clearly infringing domains held by the defendants and several examples of alleged kiting.[6]

Tasting has been the subject of a resolution from the ICANN Board and of a resolution from its GNSO Council (which develops policy with respect to .com, .net, and other gTLD domain spaces). The Board resolution was enacted with the 2007-08 ICANN budget cycle, and was effective as of July 1, 2008. It made nonrefundable the portion of each registration fee that is paid to ICANN, currently 20 cents, for all registrations over a 10 percent threshold per registrar, per month. The GNSO resolution, when implemented by March 31, 2009, will make the entire registration fee nonrefundable for any registrar that deletes more than 10 percent of its net new registrations in any month.

These resolutions each are intended to end commercial domain tasting and kiting. The Board resolution resulted in an 80 percent decline in tasted registrations the first month that it was implemented.[7] At least two large-scale tasting operations continued, however, despite the additional cost.[8] Moreover, a few conglomerates control more than 100 ICANN registrar accreditations each, so there is fear that commercial tasting still can occur by spreading a number of "free deletes" among many registrar accreditations. The GNSO Council will monitor this.

When both are implemented, these resolutions should slow the pace of new infringing registrations by making tasting harder to accomplish at scale. Yet they do nothing to address the millions of infringing registrations existing now, most having been tasted and proved profitable to their registrant. They do nothing about the ease with which newly registered and infringing domains can be monetized or about the high cost of filing a UDRP action. Of course, they do nothing to address the certain influx of many new cybersquatted registrations in the hundreds or thousands of new TLDs that ICANN will authorize in the near future.

Therefore, the cybersquatting problem is likely to continue to grow unless and until ICANN implements a policy that actually deters this insidious practice.

Phishing and Malware Distribution

Increasingly, domain name registrants are serving malware to unwitting visitors who accidentally arrive at their domains or who are driven there by spam, DNS poisoning, and other diversionary tactics. Malware comes in many forms, but typically it allows the domain registrant and its accomplices to steal personal information and money from the visitor. Malware can also turn the visitor's computer into a bot that can be remotely directed to serve spam or far worse. Botnets are often used for child porn distribution, distributed denial-of-service (DDOS) attacks, phishing, and other criminal operations.

The number and level of sophistication of phishing attacks continues to increase.[9] Classic phish attacks use spam email, designed to look as if from a trusted financial institution, to lure recipients into opening the email or clicking on a link purportedly to the financial institution's Web site. Upon opening the email or clicking on the link, the user might receive malware, which can capture their financial information. Or once at the fake Web site, the user might enter his or her user name and password and thereby transmit it to criminals. Criminals exploit the DNS by registering domains, often using stolen credit cards for payment to avoid identity detection, and then using them to send spam and host fraudulent and/or malware distribution sites.

Once these scams are detected, financial institutions and their security vendors work feverishly to have the Web site shut down. Typically, this involves notice to the Web host or other ISP if it can be located. Even when located and action is taken, however, the fraudulent site can then be moved to a different Web host or ISP, and the domain pointed to the new site. "Fast flux" name server and/or IP address changes can happen in seconds, effectively moving the Web site around to make

it impossible to take down. The only way to stop this cycle is to stop the resolution of the domain name used as a phishing lure.

Unfortunately, that is not a realistic remedy in many situations, for example when the site is hosted at MySpace, Yahoo! GeoCities, or some other shared hosting environment. Otherwise legitimate sites like these often are hacked by phishers, who then use the legitimate sites to launch phish attacks and/or malware exploits. Anti-phish teams contact the owners of hacked sites to explain the situation and how the vulnerability can be fixed. Usually a site owner is eager to try to fix the problem since it involves a breach of its site security.

This remedy takes time, but probably is the most fair and effective way to address the problem of phish attacks launched from hacked domains. The prominent shared hosting environments, including MySpace and Yahoo!, have become very effective at detecting phish sites and otherwise quickly responding to phish complaints. Yet, many Web sites fail to adopt even minimal security precautions, and a compromised Web server from an otherwise legitimate site provides a valuable distribution tool for the phisher. As a result, phishers increasingly are hacking any site they can.

In many other situations, however, the domain is used solely for fraudulent activity. Sometimes the domains are obvious trademark infringements like *pay-pal.com*. More often they are simply junk domains like *aaefraf.com*, which are then masked to visitors and spam recipients who do not realize that the actual landing URL is different from the one that they see in their browser address bar or Web link. While many domain registrars and registries will take action upon complaints and after conducting their own investigation, other registrars and registries will not act or even investigate.

Domain registrars generally are low margin businesses, and many registrars (and their downstream resellers) have no customer service to contact. So, while each may profit from every registration, many are not willing to assume the cost of customer service to address obvious abuse. That needs to change, especially as the name space expands significantly in the near future.

New TLDs and IDNs

In 2010, ICANN will usher in another wave of new TLDs, such as .web, .berlin, .sport, and .africa, which is expected to create an influx of several hundred applications.[10] ICANN staff has reported that there is no technical reason that the root zone of the Internet could not support more than 60 million new TLDs![11] Each new TLD brings the potential likelihood of systemic cybersquatting and other DNS abuse, as has been seen in all unrestricted TLDs launched to date.

For example, even today there appear few active (non-PPC parked) Web sites in .biz, in comparison to the number of domains registered, and .biz launched in 2001. Trademark owners have dutifully paid for their defensive registrations in .biz for years, many after paying to register their IP Claims with the .biz registry when it launched for the privilege of keeping clearly infringing domain names away from a competitor or infringer. They have done the same in .info and other unrestricted gTLDs, as well as many ccTLDs.

Several well-known brand owners have had significant success extracting settlements from large-scale squatters, and this trend may continue as the squatters' portfolio values grow and they have more to fear from adverse judgments.

Now, International Domain Name (IDN) registrations are becoming more prevalent. These are domains in scripts other than ASCII characters, such as Cyrillic, Chinese, Japanese, Korean, Arabic, and Hebrew. IDNs have been available for registration at the second level[12] and beyond for many years. But relatively few Internet users had the knowledge and technology to use them. That is changing, particularly with Microsoft's Internet Explorer version 7 incorporating IDN functionality. Trademark owners are registering IDN versions of their marks as domains, but still these alternative scripts provide ample opportunity for cybersquatters, phishers, and other miscreants to practice their craft.

Next year, there likely will be top-level IDN names introduced as new TLDs. The uptake of IDNs marks huge progress for the Internet, as it allows more people to interact in their native language. But it also is a serious concern because law enforcement efforts are already overburdened and certainly ill equipped to deal with domains in non-ASCII scripts. It is also expected that many users of IDN domains will be relatively new to the Internet and thus more easily victimized by online criminals. To be sure, trademark owners have much to be concerned about the growing popularity of IDNs and the prospect of dozens or hundreds of new TLDs in the near future.

Defensive (aka sunrise) registration schemes have been used in previous TLD launches to mitigate cybersquatting, but they are not sustainable across many more new TLDs. ICANN registrars and registries, by offering trademark terms to their owners ahead of land rush registrations to the general public (and then complying

with UDRP decisions), have thought that they did enough to prevent cybersquatting, while profiting from every defensive and infringing registration. But this has failed to deter wide scale cybersquatting and has led to unfair and recurring costs to brand owners for defensive registrations. This sunrise scheme is surely not scalable across many new TLDs.

Most trademark owners will not pay to defensively register in many, if any, new TLDs because the value of holding these domains in previous TLDs largely has been disproved. Instead, many more are likely to invest in infringement monitoring services, cease-and-desist notices, and in legal action against infringers and their accomplices, likely including registrars and registries (and perhaps also ICANN) as defendants more often. Several well-known brand owners have had significant success extracting settlements from large-scale squatters, and this trend may continue as the squatters' portfolio values grow and they have more to fear from adverse judgments.[13]

Ideally, ICANN can develop policy that deters abusive registrations, rather than allowing courts around the world to decide various rules to deal with ICANN and its contracting parties' registration practices.

Policy to Address Abusive Registrations

Today, other than the UDRP, ICANN has no policy in place to deter or prevent abusive registrations in existing or new TLDs. Yet, while difficult to quantify, the abusive-registration problem is undoubtedly enormous and growing. In this increasing threat environment, at minimum ICANN needs to implement a policy to end commercial domain name tasting and kiting (as it has resolved to do). That should slow the flow of new cybersquatting cases but will do nothing with respect to phishing or malware, for example. ICANN further must explore limits on fast flux DNS changes, should consider minimum response requirements for registrars and registries to address complaints of abuse, and ought to adopt a policy that allows registrars and registries to suspend DNS to clearly abusive domains.

Certainly the cybersquatting problem has morphed over time such that the existing UDRP remedy is ineffective in the face of the massive volume, speed, and sophistication of many modern trademark cybersquatters. It was enacted at a time when domain registrations cost at least $50, and cybersquatters profited primarily by selling domains to trademark owners or to other squatters. Today, domains are often less than $10, and squatters can register thousands of domains in minutes and then immediately monetize traffic via pay-per-click and other forms of advertising. Many trademark owners have more domain name registrations and more domain name infringement matters than they can manage. Most of their registrations have been recovered from squatters or have been defensively registered to keep from squatters. Few trademark owners have any appetite to buy still more domains, from either squatters or registries.

Of course, the UDRP was never intended to deal with phishers and drive-by downloaders, much less IDNs or new TLDs. Yet the DNS is increasingly abused by criminals, and IDNs and new TLDs open up huge new namespaces for criminal and cybersquatting activity. Domain registration systems allow essentially unauthenticated purchases, and then permit automated fast flux DNS exploits that make it impossible for law enforcement to detect and stop a huge amount of criminal activity. The anti-phishing community has witnessed, time and time again, massive abuse against one registry or registrar that has a vulnerability. Once the vulnerability is fixed, the criminals move on. Once hundreds or thousands of new TLDs are launched, criminals will have many more targets to exploit.

Many ICANN-accredited registrars and registries make efforts to deal with these problems on their systems, yet some do nothing. As it stands today, too many refuse to act and instead knowingly profit from illegal activity. ICANN has accredited nearly 1,000 different registrar entities, many of which resell their services through hundreds or thousands of affiliates. Too many of these vendors have no or minimal customer service to respond to abuse complaints. There could and should be a minimum response process for registrars to respond to complaints, limits on the ability of registrants to change their IP addresses and name servers, and a process for registries to take action in the event that their registrars have not.

ICANN has begun to look at how it might address fast flux DNS exploits. The Security and Stability Advisory Committee (SSAC) issued an advisory about the problem in March 2008,[14] and in May 2008 the GNSO Council resolved to form a Working Group to consider the issues around fast flux hosting and whether ICANN contracting parties could help to mitigate criminal DNS exploits. This Working Group issued its initial report for public comment in January 2009.[15] It is expected that the GNSO process will take at least three more months before any resolution, and then it will take three to six months for implementation of any resolution.

ICANN is also looking at registration abuse policies of its contracting parties. The GNSO Council has recognized that such policies are inconsistent among the contracting parties.[16] The ICANN staff has published an Issues Report outlining further work to be done as a precursor to a formal policy development process (PDP) under the ICANN bylaws.[17] The Council has

commissioned a Working Group to perform that work this spring. Indeed, the entire new TLD program has been delayed at least six months (with applications not expected to be allowed before January 2010), as ICANN promises to address the overarching issues of trademark infringement and DNS exploitation in new TLDs through consultation with Internet community stakeholders and appropriate policy development.[18] In addition, the SSAC has issued its Advisory 038, which recommends that registrars provide a public point of contact for abuse matters and has asked for coordination with the Registration Abuse Policies Working Group recently commissioned by the GNSO.[19]

Meanwhile, the Anti-Phishing Working Group[20] has been working with registry representatives to develop domain name suspension processes for domains used in phish attacks. Generally, only domains that are used solely for phishing or malware distribution would be eligible for suspension; domains resolving to shared hosting environments generally would not be eligible. Only accredited anti-phishing teams would be able to file a suspension request, after taking specified steps to verify the criminal behavior. If the registrar or registrant have not remedied the problem within a certain time, then the registry would suspend the domain, and the registrant could then appeal. It is hoped that this process will prove effective in minimizing false-positive complaints and also in minimizing the time that domains are kept live during active phish or malware attacks. If it proves effective, then it could be adopted voluntarily by other registries and might be adopted as a Consensus Policy applicable to all.

This sort of take-down decision is made every day by many ISPs, registrars, and registries, but they are not made quickly, uniformly, or often enough. These parties all fear liability in the case of a wrong decision in which a legitimate Web site is taken down. While that may be a real concern, there never appears to have been a lawsuit against a registrar or registry for doing so, and relevant, industry-standard contractual provisions—between ICANN and registries, registries and registrars, and registrars and registrants—already clearly prohibit abuse of a domain in violation of third-party rights. So this should provide cover in the rare event of a false-positive domain suspension, done in good faith to protect the public from crime, which can be quickly reversed in case of error.

The harm of temporarily suspending a legitimate Web site pales in comparison to the massive and growing harm caused by criminally abusive domain registrations, materially assisted by ICANN contracting parties and indeed by ICANN itself. These parties should not be allowed to continue to take revenue from clearly abusive registrations without policies in place to deal with complaints of abuse. Just as search engines and other online marketplaces have had to adopt trademark and other policies to deal with illegal activity on their systems, ICANN's contracting parties must evolve to do the same. This will result in a safer and more profitable Internet for everyone.

Notes

1. The Verisign Domain Report, "The Domain Name Industry Brief," Vol. 5, Issue 5, (Dec. 2008) at 2, *http://www.verisign.com/static/044349.pdf.*
2. *E.g.*, World Intellectual Property Organization, IP Services, Domain Name Statistics, "Total Number of Cases per Year," *http://www.wipo.int/amc/en/domains/statistics/cases.jsp*; World Intellectual Property Organization, IP Services, Domain Name Statistics "Case Outcome by Year(s) (Breakdown)," *http://www.wipo.int/amc/en/domains/statistics/outcome.jsp*; Laura MacInnis, "U.N. Agency Ousts Record Number of 'CyberSquatters,'" *Reuters*, Mar. 27, 2008, *http://www.reuters.com/article/technologyNews/idUSL27502002008032 7.*
3. MarkMonitor, "Brandjacking Index" (Summer 2008) at 8 and 13, *http://markmonitor.com/download/bji/BrandjackingIndex-Summer2008.pdf.*
4. *See* Phil Lodico, "Deriving Value from Web Sites: Search Engine Marketing, Search Engine Optimization, and Parking," INTA, Trademark Law and the Internet 2009, *http://inta.org/meeting_portals/09TLI/cm/Follow_the_Money-Lodico.pdf.*
5. *See* Mike Rodenbaugh, Patrick Jones, & Olof Nordling, "Outcomes Report of the GNSO Ad Hoc Group on Domain Name Tasting," Oct. 4, 2007, *http://www.gnso.icann.org/drafts/gnso-domain-tasting-adhoc-outcomes-report-final.pdf.*
6. *See, e.g.*, Mike Masnick, "Dell Sues Cybersquatters for Elaborate Shell Game," *Techdirt*, Nov. 29, 2007, *http://techdirt.com/articles/20071129/015252.shtml*; Kevin Kingsbury, "Verizon Wins Suit Over Internet Addresses," *Wall St. J.*, Dec. 26, 2008, *http://online.wsj.com/article/SB123013196536432935.html*; Anne Broache, "Luxury Retailers Go After Alleged Cybersquatters—Again," *Cnet News*, Mar. 23, 2007, *http://news.cnet.com/8301-10784_3-6170192-7.html.*
7. ICANN, Announcement, "AGP Deletes Down by 84 percent," Nov. 13, 2008, *http://www.icann.org/en/announcements/announcement-13nov08-en.htm.*
8. Posting of Mike Rodenbaugh to *http://gnso.icann.org/mailing-lists/archives/council/msg05729.html* (Nov. 19, 2008, 17:19:28).
9. Anti-Phishing Working Group, "Phishing Activity Trends Report Q2/2008," April-June 2008, *http://www.antiphishing.org/reports/apwg_report_Q2_2008.pdf.*
10. *See* ICANN, Topics, "New gTLD Program," *http://www.icann.org/en/topics/new-gtld-program.htm.*
11. ICANN Staff Draft Paper, "DNS Stability: The Effect of New Generic Top Level Domains on the Internet Domain Name System," Feb. 6, 2008 at 4, *http://www.icann.org/en/topics/dns-stability-draft-paper-06feb08.pdf.*

12. .com is a TLD, yahoo.com is a second-level name, yahoo.co.uk is a third-level name.
13. *See, e.g.*, Masnick, Kingsbury, and Broache, *supra* n.6.
14. ICANN Security and Stability Advisory Committee, "Advisory on Fast Flux Hosting and DNS: Fast and Double Flux Attacks," SAC 025, Mar. 2008, *http://www.icann.org/en/committees/security/sac025.pdf.*
15. Initial Report of the GNSO Fast Flux Hosting Working Group, Jan. 26, 2009, *http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-initial-report-26jan09.pdf.*
16. Motion Proposing an Issues Report on Aspects of Registry-Registrar Agreements, Sept. 25, 2008, *http://gnso.icann.org/resolutions/#200809.*
17. Marika Konings, "GNSO Issues Report on Registration Abuse Policies," Oct. 29, 2008, *http://gnso.icann.org/issues/registration-abuse/gnso-issues-report-registration-abuse-policies-29oct08.pdf.*
18. Draft Applicant Guidebook: What You Told Us, Feb. 18, 2009, *http://icann.org/en/announcements/announcement-3-18feb09-en.htm.*
19. SAC 038: Registrar Abuse Point of Contact, Feb. 25, 2009, *http://www.icann.org/en/committees/security/sac038.pdf.*
20. The APWG is a wholly separate entity from ICANN, though part of its mission is to influence ICANN policies relevant to the anti-phishing community, particularly through its Internet Policy Committee.