

Tuesday, August 31, 2010

Zak Muscovitch for CIRA Board

It's that time of year again when CIRA holds it's elections for seats on the Board. As I never tire of relating: when I was on the CIRA Board, I got the opportunity to travel across the country and meet .CA domain holders from all walks of life. When the Board held open forums in various venues, the turnout was usually pretty good, and people had a lot to say. Then, near the end of the forum I would always ask the room: Who here voted in the last CIRA election? Very few hands would go up.

The .CA space is unique in that it is one of the very few top-level domains that provide direct member input via the public consultations and the Board elections. I think all interested parties should avail themselves of that opportunity.

Every year the CIRA members (that's pretty well anybody who holds a .CA domain name) can put one candidate onto the ballot, in addition to the slate of candidates proffered via the CIRA NomCom (Nomination Committee). The member nominees this year are numerous, and I recognize a few names there. It's a shame we can only show our support for one member nominee at this stage of the game.

So, who should you support from the members' side of the slate this year?

My overall number one choice is Zak Muscovitch, a domain name lawyer and all around advocate for domainer rights. I've had numerous dealings with him in the past and he's very plugged in and attuned to the domain name space. He's also written some groundbreaking articles about reverse hijacking.

If your main concern about the .CA space is around technical stability and security, I would look at Andrew Sullivan, a long time DNS guru who I've turned to for advice and guidance in the past.

And if you're looking for an all around generalist with a good head for numbers and a down-to-earth grounding then I see that Rick Anderson is running on the member's side of the ledger this year. He's been on the Board before and I thought it was well served by his presence.

Posted by easyDNS: of Interest in via easyDNS blog at 11:40

Thursday, August 19, 2010

DOS Attacks and DNS: How to Stay Up If Your DNS Provider goes DOWN

Greetings from St. Lucia, where I'm here with the family for an end-of-summer vacation. I wanted to post about this topic before I left but I didn't get to it, but this article over at CircleID reminded me. The article discusses the ramifications and effects of the large, possibly record-setting DOS attack against DNSMadeEasy last weekend. (To clarify: DNSMadeEasy is a separate company, unrelated to easyDNS) The article states "An attack on DNS is an attack on The Internet" and this much is true. As we always quip around here, "DNS is something nobody notices until it stops working". I have to admit that in the early days of easyDNS I was oblivious to the possibility of DOS attacks. It simply never occurred to me. We were able to proclaim 100% DNS uptime since launching in 1998 for a glorious 5 years and then on April 14th, 2003, it all ended as we got hit with a DOS that pancaked all four single-node nameservers and every domain on the system went dark for about 75 minutes. I nearly had a nervous breakdown, and then over the summer I thought long and hard about the ramifications and at the time surmised that the DNS hosting model was doomed.

Then we started looking at DNS anycasting but it took us another 5 years to get there. In the meantime we had another outage from another DOS: about an hour on Sept. 14/2005. We added Prolexic DDoS mitigation within weeks of that attack and are happy to report we haven't had an outage since. In the intervening years we also moved ourselves to a DNS Anycast architecture. While it is significantly harder to bring down an anycast architecture with a DOS attack, it can still happen. Usually instead of a complete and utter outage, you get "regional outages", which is basically a euphemism to deflect assertions of downtime: "Some users may experience regional outages, like North America and Europe" (credit to Steven Job for that bit of humour). Some DNS Providers guarantee you that they will never go down and assert 100% DNS uptime in face of prior DOS attacks. In reality, every single DNS provider in existence for more than 5 years has had downtime. If the DOS attack that hit DNSMadeEasy last week really was 40 or 50 GIGS, and if it would have hit us, I hesitate to say "we would have stayed up". In 2006 we got hit with an attack that was 20 to 25 gigs, and we didn't go down completely ("Some customers may have experienced regional outages"), but we sure felt it. Prolexic withstood the attacks and at the end of it we had to write a few enormous cheques to our providers to cover the bandwidth. But I have long since backed away from my 2003 trepidations that the centralized DNS hosting model was doomed, for a few reasons:

DNS Anycast changes the game and drastically raises the bar for a DOS attack so that even if the resources can be mustered to do it, the duration of an outage is usually decreased as more numerous network carriers become aware of the problem and act to corral it.

DDoS Mitigation strategies have also improved. These days I think we are pretty well under a continuous state of low intensity DOS attack in one form or another. By low intensity I mean it doesn't bring us down anymore, but these attacks are about 10 to 20 times more powerful than the 2003 attack that did us in, so:

The DOS attacks that DNS providers routinely mitigate every day would probably level many non-professional, non-dedicated DNS setups.

The other benefits to using an specialized DNS hosting provider outweigh the isolated risks of DOS attacks. A good example of this is DNS Anycast: the DNS best practice that is simply not-viable for many organizations to implement on their own. Commercial DNS providers make viable through their economies of scale.

But this is the internet. If you elect to take part in it, there are certain unpleasant realities that will come home to roost. Like if you own a domain name, sooner or later it'll get joe-jobbed in a spam mailout. So to eventually you will get caught in the crossfire of a DOS attack against some target that has nothing to do with you but it's big enough to mess up one of your infrastructure suppliers. Like an empty bottle thrown at random into a crowd.

On the DNS side of things there are a few steps you can take to either not go down, even if your DNS provider does, or to make any impact minimal.

Use a DNS provider that allows third-party zone transfers. Either one that lets your slave your DNS zone from a primary nameserver outside of their own system (basically using a DNS provider as secondary DNS), or one that lets you designate other nameservers outside their system that can slave your DNS zone from it. Ideally, both.

Use two DNS providers. If you have the ability to setup a point #1 above with multiple DNS providers, then you are pretty redundant right there. I got an email from a large web services company after the DNSMadeEasy DOS who uses both theirs and our services. He said they experienced no downtime and using two DNS providers was still a lot less expensive than their previous setup.

Or, just use any third party nameserver, even one of your own. Have it slave your zone from your DNS host (or have your DNS host slave from it). Unless you are the actual target of the DOS, then, like a jet that can fly as long as one engine is firing, you'll be fine for the brief time your DNS provider may be down (or experiencing regional outages).

Being connected to the internet has varying degrees of importance to different organizations. For some, no downtime is acceptable (i.e. for DNS providers or web hosts, it's very very bad). Other organizations take a couple years to notice that their domain name expired.

Depending on the seriousness of your web presence you may want to also consider additional measures and be aware of a few things.

Many top-level rootzones (.com, .net, .org, .biz and .info) make modifications in near realtime. People may be accustomed to things like nameserver delegation modifications to take a day to kick in. In fact a lot of user-interface verbiage probably still says as much ("please allow 24 to 48 hours for your nameserver delegation to take effect"). In these rootzones it's closer to 3 to 5 minutes. Use that. The bad guys (spammers, botnets, etc) "fast-flux" their nameservers all the time to thwart tracing and reporting. It's a tactic you can take back from the black-hats and you can fast-flux your nameservers to provide a moving target in a DOS situation.

Warm spares: have your DNS mirrored on third party nameservers, but do not add them to your nameserver delegation. If your DNS provider goes down, you then temporarily swap in your warm spares.

For web hosts or other infrastructure suppliers that run DNS for their clients: do the above, except when you need to make a switch to your warm spares, you change the rootzone glue record for your nameservers: this way you do not need to make changes to each customer domain's nameserver delegation. The caveat here is you tend to only buy time: if the DOS is targeting you and you change-up your nameserver glue, the DOS may eventually (or sooner) follow you to the new IPs. Having said that, you can keep doing this and you may be able to diffuse the attack.

Another overlooked fact: you can round-robin a nameserver glue record. We've tried it and don't find it near as effective as DNS anycast, but in a DOS situation, if you can add more warm spares to your nameserver glue records, then do it. Again, this diffuses the attack. "Regional outages" may indeed be a euphemism but it really is better than "everything is down hard".

Here's one we learned the hard-way: don't have your nameservers in the same netblocks as your web interface and data storage, especially if you provide infrastructure services. If your nameservers are going to get clobbered you at least want to be able to get email and maybe provide a modicum of critical services to your users, something you can't do if your entire operation is within the same /24 that has been null routed by your upstream providers.

If I can perhaps add some comments to this theme: I would not wish a nameserver outage on any DNS provider. And you can believe me, when it happens, the people inside that company are tearing their hair out, suffering extreme mental anguish and pulling out all the stops to restore services. When I see a DNS provider taken out by a DOS attack and chatter on twitter, etc along the lines of "XYZDNS is down #fail #fail #fail" I want to thwap those people upside the head. Get a life. Do you think your DNS provider is out on the golf course while his business is being taken apart by a DOS?

While I am a businessman and we are a for-profit company, I do not relish gaining business at the expense of a DNS provider who's down because of a DOS attack. I'd rather gain customers on price, service offerings, customer support, our good looks, anything but a competitor going down because of a DOS. I guess because I've been there, I know how it feels. (Not all DNS providers take this view, in fact some of them pounce with glee when the opportunity presents itself, firing up the telemarketing crew to cold call the fallen provider's customers. If you're a customer of ours you have perhaps received such a call in the past).

DOS attacks are criminal acts. Get pissed off at the criminals who undertake them, not the people who are on the front lines of having to deal with them. Use these tips to stay online regardless of who your DNS provider is. I'm not advocating you stop using your existing DNS provider, but rather you modify your tactics so that instead of your DNS host becoming your single DNS host, it becomes more of a "DNS infrastructure management" role, that you use to setup and maintain multiple DNS structures (combining in-band nameservers from your DNS host with out-of-band nameservers outside their cloud), and warm spares.

Posted by easyDNS: of Interest in via easyDNS blog at 11:49

Thursday, June 3, 2010

tweet2txt? tweet2dns? ok, why not!

Not even sure why we did this other than "because we could", but try this:
Setup a txt record in your domain like this:

```
host IN TXT ""v=twitterstatus1 txthost twitterid"
```

And basically what happens is the last tweet from "twitterid" will be placed into the contents of a TXT record for "txthost" under your domain name.

Kind of like a tweet2txt or tweet2dns gateway.

So now in the above cases:

```
markjr@c3po:~$ host -t txt mark.jeftovic.net
mark.jeftovic.net descriptive text "Ok, about to announce tweet2txt or tweet2dns via the company blog...."
and
```

```
markjr@c3po:~$ host -t txt markwork.jeftovic.net
markwork.jeftovic.net descriptive text "Ok, the final word on DNS pricing is up (pricing for heavy use domains over 5 million queries per month) http://easyurl.net/dnspricing"
```

These get refreshed every 5 minutes.

This is of course, of no practical value at this point in time. But it opens the door to bridging the gap between your social network status and your personal domain's DNS and who knows, maybe somebody will do something interesting with that.

Posted by easyDNS: Tips and Tricks in via easyDNS blog at 14:20

Thursday, May 13, 2010

An iPhone hack for dynamic DNS updates with easyDNS

File under neat.

Gavin Brock posted a way to dynamically update your DNS for your (jailbroken) iPhone. This is the same Gavin Brock who wrote the DNS::EasyDNS Perl Module many years ago.

Posted by easyDNS: Tips and Tricks in via easyDNS blog at 10:10

Sunday, March 28, 2010

When RBLs go bad: blackholes.uceb.org is now wildcarded

blackholes.uceb.org was an antispam RBL that shut down in 2008, but as with all RBLs, they tend to find their way into mail server configs and then ossify there.

It looks like whoever ran uceb.org decided that two years was enough and to let the domain lapse. Yesterday, the domain's registrar put the domain in a "pending delete or resale" status:

Domain ID:D84712302-LROR

Domain Name:UCEB.ORG

Created On:21-Mar-2002 11:13:47 UTC

Last Updated On:27-Mar-2010 08:19:20 UTC

Expiration Date:21-Mar-2011 11:13:47 UTC

Sponsoring Registrar:Network Solutions LLC (R63-LROR)

Status:CLIENT TRANSFER PROHIBITED

Status:AUTORENEWPERIOD

Registrant ID:DOMAIN-RESALE

Registrant Name:Pending Renewal or Deletion

and then, as is pretty standard operating procedure in cases like this: they wildcarded the domain's DNS.

That means for anybody who was still referencing blackholes.uceb.org in their mailer config, it wasn't doing much damage (or good) since July, 2008 until yesterday. Then they probably started rejecting ALL email because all addresses within *.blackholes.uceb.org now return true;

Posted by easyDNS: of Interest in via easyDNS blog at 16:37

Thursday, March 4, 2010

.CO Domain Registrations are Coming. Will You Participate?

A bunch of years ago I had an idea for an espionage/action/thriller story where a bunch of mercenaries planned a coup d'etat against the regimes of either Columbia or Cameroon for the sole reason of gaining control over the country's top-level domain registry and making billions off of typo-squatting .COM.

Truth did kind of mimic fiction (minus the coup d'etat part) when Kevin Ham cut a deal with Cameroon to wildcard .CM root. Well now Columbia has decided to overhaul it's .CO root level domain and open it up to second level registrations for non-locals.

.CO is being marketed ostensibly as 'Associated globally with the words "COmpany," "CORporation" and "COmmerce"', but let's face it, the activity in this TLD is going to be driven primarily by the fact that it's a typosquatter's wet dream for .COM and a goddamn headache for everybody else with a net presence built mainly under .COM.

As we've observed before (here and then here), most registrars like to whip their customer base into a frenzy to "grab your name" under every TLD that tries to tart itself up as some pseudo-generic and trots itself out as the latest "must-have" domain. Most of them aren't "must-haves" and a lot of them are quite frankly, a waste of time and money.

So it is with a heavy heart I have to come out and say this. If you're operating a serious net presence on .COM, you probably should go out and get the .CO version of your name, as much of a royal pain in the ass as that is/will be. Not to mention expensive. The base cost on a non-Columbian Sunrise claim will be somewhere north of \$250 (non-refundable) and for landrush there will be a small non-refundable "application fee" but the first year registration will be over \$200. Then after landrush, the cost will settle down to a more digestible level, only about 3 times the wholesale base cost of an actual .COM.

Nice work if you can get it.

We don't want to make a bad situation worse, but we won't work for free either, so we'll try to keep our markup reasonable.

What I am interested in is what our members think of this. If you have a few moments, please take the following survey on whether you will participate in .CO. For each response we'll donate \$1 to the charity of your choice.

Feel free to comment as well. Continue reading ".CO Domain Registrations are Coming. Will You Participate?"

Posted by easyDNS: Domain Industry Watch in via easyDNS blog at 21:44

Blog Export: Exile From the Herd, <http://www.privateworld.com/>

Tuesday, September 1. 2009

easyURL.net now CLOSED to general public

Our URL shortening service easyURL.net is now CLOSED to the general public. Only easyDNS members in good standing with at least one active domain in their account may use this service. To enable your access log into your easyDNS account and under your utilities module click on enable easyURL.net and then you're done. Happy shortening. Everybody else can make other arrangements. Thank you for your time.

Posted by easyDNS: of Interest in via easyDNS blog at 14:19

Blog Export: Exile From the Herd, <http://www.privateworld.com/>

Tuesday, August 18, 2009

easyURL.net adds useless "easyFrame" to redirects.

Feeling left out of the web 2.0 "URL Shortener" hysteria, we've added a mostly useless "easyFrame"(tm) to the easyURL.net redirect service. The culmination of nearly two night's worth of programming in front of the TV, and nearing 100 lines of PHP code, the easyFrame(tm) enables people to further perpetuate it's marginal functionality via other social networking sites with a single click. Users may also "vote" on whether they actually like or dislike the subject URL being shortened.

Perhaps the single actual useful function of the easyFrame(tm) is that you can also report spam URLs directly to us, with one click, which we will then nuke with extreme prejudice.

We are also happy to report that our new easyFrame(tm) has enticed a VC bidding war and easyURL has closed a \$30 Million dollar A series funding round with a pre-money valuation more than 100X that of easyDNS itself. We are now planning on spinning off easyURL.net in an October IPO.

Try it today! Tell your friends! Tweet it!

Posted by easyDNS: of Interest in via easyDNS blog at 23:43

Saturday, May 30, 2009

Whois Privacy brings a lawsuit down on Registrar

Following on our explanation of why we do not offer whois masking here at easyDNS, we note tonight that Registrar Namecheap has been sued "over cybersquatting claims for a domain name registered under the NameCheap whois privacy services".

As we outlined in our original article: Whoever is listed as the Registrant in the domain's whois record, effectively owns the domain. If you own the domain, you get all the responsibilities for it. That's why most Registrars simply drop the whois mask at the slightest legal speedbump. Namecheap didn't, and so now it cuts the other way they get the sharp end of the legal stick being poked at the domain.

Technology lawyer Eric Goldman in his analysis of the matter under the subheading Why This is a Troubling Ruling noted: Read literally, every proxy service is exposed to potential contributory ACPA liability for every domain name it services. I can't imagine proxy service providers will be excited about that liability exposure, and some may choose to exit the business.

Some certainly should. Any of the proxy providers who basically viewed whois masking as an easy business which basically pulls in money for doing nothing (which is more or less how I view it, I'm sorry, but that's only my opinion) - should take this as their signal that the party's over and exit the business.

As I've noted before, in it's current implementation: whois privacy doesn't actually protect the underlying registrant's privacy (because most proxy providers will drop the mask at the first sign of trouble) and if they don't, the proxy providers are exposing themselves to inordinate risk. Coupled with the fact that the whois mask puts the underlying registrant's rights to the name in question and the whole thing is just one big mess waiting to blow up.

Posted by easyDNS: Domain Industry Watch in via easyDNS blog at 09:30

Friday, May 29, 2009

Whois Privacy brings a lawsuit down on Registrar

Following on our explanation of why we do not offer whois masking here at easyDNS, we note tonight that Registrar Namecheap has been sued "over cybersquatting claims for a domain name registered under the NameCheap whois privacy services".

As we outlined in our original article: Whoever is listed as the Registrant in the domain's whois record, effectively owns the domain. If you own the domain, you get all the responsibilities for it. That's why most Registrars simply drop the whois mask at the slightest legal speedbump. Namecheap didn't, and so now it cuts the other way they get the sharp end of the legal stick being poked at the domain.

Technology lawyer Eric Goldman in his analysis of the matter under the subheading Why This is a Troubling Ruling noted: Read literally, every proxy service is exposed to potential contributory ACPA liability for every domain name it services. I can't imagine proxy service providers will be excited about that liability exposure, and some may choose to exit the business.

Some certainly should. Any of the proxy providers who basically viewed whois masking as an easy business which basically pulls in money for doing nothing (which is more or less how I view it, I'm sorry, but that's only my opinion) - should take this as their signal that the party's over and exit the business.

As I've noted before, in it's current implementation: whois privacy doesn't actually protect the underlying registrant's privacy (because most proxy providers will drop the mask at the first sign of trouble) and if they don't, the proxy providers are exposing themselves to inordinate risk. Coupled with the fact that the whois mask puts the underlying registrant's rights to the name in question and the whole thing is just one big mess waiting to blow up.

Posted by easyDNS: Domain Industry Watch in via easyDNS blog at 22:26

Tuesday, March 31, 2009

Do you really need to register your name under .tel?

We've turned up .tel registrations now that they've gone realtime and the initial registry implosion has stabilized. You may have noticed a distinct lack of urgency from us to light a fire under your keester to go register your name under .tel right now before somebody else takes it.

As we outlined previously, we find the hoopla around new top-level domain rollouts both tiresome and for the majority of domain holders, unnecessary. So we have a policy here that we generally a) don't launch the new TLD until it goes realtime and is considered "stable" and b) we don't try to whip our users into a hysterical frenzy ahead of time to register their domains under every new TLD.

The fact is, in the future there will be more top-level-domains, a lot more. So many of them that between obvious typos of one's domain, one's core domain or domains, and one's local geographic top-level domain, it will be a fool's errand to try and register your name under every new TLD that comes along just for the sake of "defending your mark".

The other problem is, .tel is severely crippled

While we do find .tel slightly unique in the realm of new TLDs because it actually exists for a reason: to cultivate internet telephony usage. This isn't some country-code ccTLD hiring out their namespace under some made-up reason (.me, .tv, .ws, et al) to draw in foreign registrants, it's an actual TLD geared toward SIP, VOIP and telephony and exists for that reason.

But .tel isn't doing anything under the space that can't be done under any other domain name with the appropriate use of SRV or NAPTR records and to actually make matters worse, you are forced to use their nameservers and your domains are under an Acceptable Use Policy which forces you to use the name for certain things (basically as a "contact" switch rather than a "content" page).

While the objective may be laudable: giving a TLD an actual raison d'être beyond "register your name before somebody else does!", we don't like that you're forced to use their nameservers and don't have total latitude with your .tel domains. It runs contrary to the ethos behind easyDNS which was, and still is to drive a stake through the heart of lock-in. (It's not like we force everybody who registers a domain through us to use our nameservers because we're an outsourced DNS host, in fact we even allow our members to mirror their DNS from our nameservers from outside DNS hosts).

As such we have not become directly accredited under .tel, instead we're supporting them through our OpenSRS reseller tag, but the functionality is transparent.

Most of you reading this probably have no compelling reason to register your name under .tel unless 1) you like the TLD or 2) you have operations in the IP telephony space that would make sense segmenting under a .tel name and 3) you don't mind the crippled functionality and lock-in.

Posted by easyDNS: of Interest in via easyDNS blog at 11:50

Wednesday, March 11, 2009

New easyDNS Member feedback survey

Many of you may not know that we have an ongoing member feedback survey where we ask for your thoughts and impressions of using easyDNS.

We try to make it as unobtrusive as possible, and for each respondent we make a \$5 donation to a charity of your choosing (World Wildlife Fund, Children's Wish Fund or Unicef).

We've recoded the survey using eSurveys.com. Feel free to give us your thoughts by taking it today.

easyDNS Member Survey

Posted by easyDNS: of Interest in via easyDNS blog at 16:13

Thursday, November 20, 2008

Why we do not offer Whois Privacy at easyDNS

We get asked this a lot: Why do you guys not offer whois masking or whois contact privacy?

The brief background on this is: whenever you register a domain name, your contact details are published in a publicly visible database called "whois", where your contact details are instantly harvested by spambots and marketers who proceed to email and postal mail you marketing offers, deceptive "domain slamming" attempts, ads for dubious products, and perhaps even telemarketing calls.

Nobody likes that, so over the years people started resorting to various tactics to protect themselves from the deluge of crap that inevitably comes with simply registering a domain name: throwaway email addresses in whois records, fake postal addresses, fake phone numbers, etc. The problem is, Registrants are obligated under their various end user agreements to provide true and accurate data (not doing so is grounds to lose one's domain), and the US even passed legislation making it unlawful to use fake contact details in a domain name registration.

Our response to this, years ago, was MyPrivacy.ca which protects your email address from being harvested from your whois records, but leaves your other data intact. We didn't see it as a revenue opportunity, in fact we made it free and opened it up to competing registrars, many of whom started recommending it to their customers. We just wanted to drive a stake through the heart of the whois spammers.

It wasn't long though, before many registrars took it a step further and created the concept of "whois masking" or "contact privacy", where all of the domain-holder contact details would be masked from the public whois. Of course, this was heralded as a "value-add" and most outfits charge extra for it.

In today's long overdue post, we're finally revealing why so-called "whois privacy" puts your domains at risk, costs you more and doesn't really protect your privacy. Continue reading "Why we do not offer Whois Privacy at easyDNS"

Posted by easyDNS: of Interest in via easyDNS blog at 11:29

Why we do not offer Whois masking at easyDNS

We get asked this a lot: Why do you guys not offer whois masking or whois contact privacy?

The brief background on this is: whenever you register a domain name, your contact details are published in a publicly visible database called "whois", where your contact details are instantly harvested by spambots and marketers who proceed to email and postal mail you marketing offers, deceptive "domain slamming" attempts, ads for dubious products, and perhaps even telemarketing calls.

Nobody likes that, so over the years people started resorting to various tactics to protect themselves from the deluge of crap that inevitably comes with simply registering a domain name: throwaway email addresses in whois records, fake postal addresses, fake phone numbers, etc. The problem is, Registrants are obligated under their various end user agreements to provide true and accurate data (not doing so is grounds to lose one's domain), and the US even passed legislation making it unlawful to use fake contact details in a domain name registration.

Our response to this, years ago, was MyPrivacy.ca which protects your email address from being harvested from your whois records, but leaves your other data intact. We didn't see it as a revenue opportunity, in fact we made it free and opened it up to competing registrars, many of whom started recommending it to their customers. We just wanted to drive a stake through the heart of the whois spammers.

It wasn't long though, before many registrars took it a step further and created the concept of "whois masking" or "contact privacy", where all of the domain-holder contact details would be masked from the public whois. Of course, this was heralded as a "value-add" and most outfits charge extra for it.

In today's long overdue post, we're finally revealing why so-called "whois privacy" puts your domains at risk, costs you more and doesn't really protect your privacy.

If you haven't seen a "whois record", go to <http://www.easywhois.com> and enter a domain name, any domain existing name, and look at the record. If you enter easydns.com you'll see our corporate contact details, our address, the legal name of our company, our phone and fax numbers.

Then enter a domain name that has "whois privacy", instead of seeing the actual end-user contact details of the domain holder, you'll see something like:

Privacy Protection or
Contact Privacy

and some other address info which is basically all a "mask".

Here's what you need to understand: Whether a domain name is considered "property" (like in .com) or just

conveys "rights" (like .ca here in Canada), the domain is considered the property of, or the rights accrue to, whoever or whatever is listed in the whois record.

If you use whois privacy and some kind of dispute arises between you and your Registrar, and you were to go to ICANN or CIRA and assert your rights to that name, they would look at the whois record details and tell you that you have no standing. The domain belongs to the "privacy entity" listed in the record.

From ICANN or CIRA's point of view, having a contract in place between you and the "privacy provider" isn't a factor, the domain belongs to them, not you. If you want to do something about it, you'll have to follow that up in court. If your Registrar (or privacy provider) is in some other legal jurisdiction, then you have that additional hurdle to deal with (that of suing a company in another country).

And that's if the Registrar is still in existence. If the reason you have a problem in the first place is that your registrar has imploded and disappeared (RegisterFly anyone?) then you have 1) nobody to sue and 2) no way to prove you are the "real" owner of all your "privacy protected" names.

It is true that Registrars are now obligated to escrow their Registrant data to protect against Registrar failure (I call this the "RegisterFly Rule"), if your whois records are privacy masked, then the data that will be escrowed will be the masked data, not the underlying registrant data.

There is nothing in the ICANN Registrar Accreditation Agreement that provisions for whois masking or privacy protection that puts an onus on the Registrar to preserve the underlying registrant data anywhere and maintain a verifiable link between the "real" record and "masked" record. There is nothing in the Registrar data escrow requirements that says a registrar has to provide the underlying "real" record to the escrow provider.

I find this risk so unacceptable that I simply refuse to sell this stuff to the public. Liken whois privacy to the "Credit Default Swaps" of the domain world. As long as nothing goes wrong, everything is fine and everybody makes money. As soon as something goes wrong, all hell breaks loose.

It gets worse: Whois Privacy only protects you from the most cursory examination of your details. In the event of an even moderate intensification of scrutiny: a UDRP challenge, a subpoena, or any legal action, you will find that the Registrar will drop your privacy mask as a matter of policy and restore your underlying live data anyway.

There are even some Registrars who will set you up with "privacy protection" on one hand, and will then sell your private data out the other side to anybody who wants it. Now I once wrote about this and was criticized for "not naming names", so if you have that same objection now, email me and I will send you a link to a page from a large Registrar who offers whois privacy protection that offers to sell you the underlying masked data for any "privacy protected" registrant on their system for \$10.

Once again, we have something that strikes me just another Registrar "cash grab" that not only doesn't provide any real benefits to the domain holder but actually adds an unacceptable amount of risk.

Posted by easyDNS: of Interest in via easyDNS blog at 11:29

Thursday, November 6, 2008

MobileMe and easyDNS...

A number of customers have been registering domains to point to their new websites published via iWeb on their MobileMe accounts. Unfortunately, while MobileMe instructs how to point "www.yourdomain.com" to their services, they don't have a way to easily point just "yourdomain.com" to their services. This is especially important as not everyone on the internet will type "www" before a domain name when looking for a website (such as "www.google.com" versus "google.com").

Realising this is an issue for some of our customers who have DNS-Only services, we have implemented a work around. Simply follow the instructions on MobileMe to have your "www.yourdomain.com" CNAME point to "web.me.com". These are correct, and are very important. However, one last step is to leave your "yourdomain.com" record in the "hosts" block pointing to the word "PENDING". It should look something like this: A record (host): yourdomain.com Has IP: PENDING

...with your CNAME looking like this: C name (alias): www.yourdomain.com Points to A record (host): web.me.com Once entered, click "next" to submit your changes, and "next" again after you have confirmed all looks well. These updates may take a few hours to propagate across the internet before you can see them.

If you have any questions at all, please contact our Support Dept., and we would be happy to assist you.

Posted by easyDNS: Tips and Tricks in via easyDNS blog at 13:03

MobileMe and easyDNS!

A number of customers have been registering domains to point to their new websites published via iWeb on their MobileMe accounts. Unfortunately, while MobileMe instructs how to point "www.yourdomain.com" to their services, they don't have a way to easily point just "yourdomain.com" to their services. This is especially important as not everyone on the internet will type "www" before a domain name when looking for a website (such as "www.google.com" versus "google.com").

Realising this is an issue for some of our customers who have DNS-Only services, we have implemented a work around. Simply follow the instructions on MobileMe to have your "www.yourdomain.com" CNAME point to "web.me.com". These are correct, and are very important. However, one last step is to leave your "yourdomain.com" record in the "hosts" block pointing to the word "PENDING". It should look something like this:

A record (host): yourdomain.com

Has IP: PENDING

...with your CNAME looking like this:

C name (alias): www.yourdomain.com

Points to A record (host): web.me.com

Once entered, click "next" to submit your changes, and "next" again after you have confirmed all looks well. These updates may take a few hours to propagate across the internet before you can see them.

If you have any questions at all, please contact our Support Dept., and we would be happy to assist you.

Posted by easyDNS: Tips and Tricks in via easyDNS blog at 13:03

Tuesday, October 28, 2008

How to explain "URLs" so anybody can understand them

One of our tech support guys just had a conversation with somebody who wanted "to register the URL <http://example.com/something.html>", where example.com was already registered, the person couldn't understand why he couldn't have that URL with "something.html" after it.

We've heard variations of this one a lot. Like somebody who knows "xyz.zz" is taken "but can I register "www.xyz.zz?", no, you can't.

The easiest way to explain a URL such as this one:

<http://www.example.com/something.html>

Is to think of it as HOW, then WHERE and finally WHAT:

<http://>

– how?

The method we are going to use to retrieve or "get to" the document described by the URL. Common ones are "http" (Hyper-Text Transfer Protocol), you may also see "ftp://" or "mailto:"

www.example.com

– where?

This is the hostname of the server, somewhere on the internet, which is holding the document we actually want

[/something.html](http://www.example.com/something.html)

– what?

Finally, after we know what server we are looking for and how we're going to retrieve the document from it, we now specify exactly which document we want off of the remote server.

Understand those three components and you basically have URLs down cold.

Your web browser (firefox, safari, IE, Opera) is all about "how", what protocols to use to pull all these documents over the web to your desktop.

The web host is the "what" machine. It sits on a server and serves document after document to remote web browsers who send it requests.

Something has to bridge the browser to the web host/server and that's the "where", that's where DNS and domains come in, and that's primarily what we do here at easyDNS. We tell web browsers (and other client applications) the "where" aspect of retrieving and transmitting documents (the "whats") across the internet. We do this via "DNS lookups" about a quarter billion times a day.

Posted by easyDNS: Tips and Tricks in via easyDNS blog at 09:47

Monday, September 29, 2008

What part of "blanket permission to download" do Michael Moore's lawyers not get?

Michael Moore released his latest film *Slacker Uprising* for free, over the web (note: don't click on that link if you live outside of the US or Canada or his lawyers will yell at us again). On the download page for the film Mr. Moore has this to say:

"I'm giving you my blanket permission to not only download it, but also to email it, burn it, and share it with anyone and everyone (in the U.S. and Canada only). I want you to use 'Slacker Uprising' in any way you see fit to help with the election or to do the work that you do in your community. You can show my film in your local theater, your high school classroom, your college auditorium, your church, union hall or community center. You can have your friends and neighbors over to the house for a viewing. You can broadcast it on TV, on cable access, on regular channels or on the web. It's completely free -- I don't want to see a dime from this. And if you want, you can charge admission or ask for a donation if it's to raise money for a candidate, a voter drive, or for any non-profit or educational purpose. In other words -- it's yours!"

So, why are his lawyers demanding we take action regarding a torrent posted on a DNS hosting client's website? We received the following takedown request via Fedex today:

Yes, he did specify "US or Canada only please", and the offending site is in Sweden (and the lawyers cited the United States Copyright Act but we're in Canada ourselves).

But really, come on folks, please tell that isn't the basis for this take down request. Anybody with half a clue knows the net doesn't work like that.

In any case, I've sent them our standard "we're not the web host, we're just the lowly DNS service", but I did point out this seeming contradiction in Michael Moore's message vs his lawyer's actions.

This smells like one big waste of time to me. A lot of billable hours being racked up for nothing here.

Update: I've gotten an email back from the law firm. Now that they understand what a nameserver is/does they have withdrawn their letter to us, but they have confirmed that their beef here is that this torrent is hosted outside USA/Canada. I've replied that they should know it is highly impractical to attempt to impose geographical constraints on otherwise freely available files but I guess they want to give it a shot.

Posted by easyDNS: of Interest in via easyDNS blog at 17:30

What part of "blanket permission to download" do Michael Moore's lawyers not get?

Michael Moore released his latest film *Slacker Uprising* for free, over the web (note: don't click on that link if you live outside of the US or Canada or his lawyers will yell at us again). On the download page for the film Mr. Moore has this to say: "I'm giving you my blanket permission to not only download it, but also to email it, burn it, and share it with anyone and everyone (in the U.S. and Canada only). I want you to use 'Slacker Uprising' in any way you see fit to help with the election or to do the work that you do in your community. You can show my film in your local theater, your high school classroom, your college auditorium, your church, union hall or community center. You can have your friends and neighbors over to the house for a viewing. You can broadcast it on TV, on cable access, on regular channels or on the web. It's completely free -- I don't want to see a dime from this. And if you want, you can charge admission or ask for a donation if it's to raise money for a candidate, a voter drive, or for any non-profit or educational purpose. In other words -- it's yours!"

So, why are his lawyers demanding we take action regarding a torrent posted on a DNS hosting client's website? We received the following takedown request via Fedex today: Continue reading "What part of "blanket permission to download" do Michael Moore's lawyers not get?"

Posted by easyDNS: of Interest in via easyDNS blog at 15:51

Wednesday, August 27, 2008

Running an affiliate program? Don't pay for sales you already had in the bag

People have tried this on us so many times I figure it must still work in many cases so after the last one I decided to post a brief note about this.

We run an affiliate program via Commission Junction, it pays \$20 per new customer acquisition. We also come up first in all major search engines for our own name: "easydns", "easydns.com", "www.easydns.com", and "easyDNS Technologies Inc". Every online business probably comes up first in Google for their own name. (If you don't, you have larger problems and you should probably address those).

Here's what I consider, if not a "black hat" PPC technique, a grey one which we're not interested in because it costs us affiliate commissions on sales we would have gotten without the affiliate ever being involved.

Here's how the scam works: Continue reading "Running an affiliate program? Don't pay for sales you already had in the bag"

Posted by easyDNS: Tips and Tricks in via easyDNS blog at 11:31

Thursday, July 31, 2008

Ten Years of easyDNS

10 years ago on this day, we removed the password block on easyDNS.com and sent out a couple of innocuous email announcements to the PHP and Mysql mailing lists announcing that we had developed a DNS management system using php and mysql and it was now open for business. We had three nameservers, 1 in our office (where the "other server", that ran everything was), one downtown in somebody else's cage at 151 Front street, and some friends of ours in Buffalo who were running an email company called chek.com let us run a third nameserver on one of their servers. That was the initial setup of easyDNS... Continue reading "Ten Years of easyDNS"

Posted by easyDNS: of Interest in via easyDNS blog at 10:25

Wednesday, July 23, 2008

DNS cache poisoning exploit released

Hi There,

There is a new DNS Cache poisoning disclosure that has been inadvertently leaked before it was scheduled to be released by Dan Kaminsky (IOActive). This is a very serious flaw in the DNS protocol that impacts caching resolvers, like the resolvers hosted at your service provider that help your workstation resolve IP addresses to domain names.

This bug does not directly impact authoritative name servers like the ones used to host your domain names at EasyDNS. Our name servers do not request answers from external sources, and rely entirely on internal cache files to offer answers. So for example, nobody will be able to change your IP information on our end. That part of the bug is unfortunately located at the caching end.

That being said; this is still a serious flaw, and we are taking this opportunity to upgrade the DNS software on our authoritative name servers to ensure that we are 100% compatible across the board with the newly upgraded caching name servers located at your Internet Service Provider. These upgrades should not impact name resolution if you are using more than one of our name servers to serve answers for your domain name (actually, please ensure that you are).

To make sure your Internet Service Provider is up to speed, you can use Dan Kaminsky's test script at DoxPora Research. If your Internet Service Provider is not yet up to speed, you may want to give them a nudge and/or change your DNS resolver configuration to a more trusted service. Update It is now making news that an exploit to this attack has been released., please see our post about our newly launched DNSresolvers.com if you are looking for safe resolvers.

Posted by easyDNS: Domain Industry Watch in via easyDNS blog at 20:52

Thursday, July 17, 2008

.ME Top Level Domain launch indicative of new TLD rollouts

We've gotten a few invitations to apply to be a .ME top-level domain registrar, to which we assigned no urgency after we took a straw poll internally and found that pretty well zero of our customers were asking for it. Today, Techcrunch reports that the .ME landrush, at least through one large operator, had degraded into a fracas. We have an unwritten policy here: new Top Level Domain roll outs are to be avoided until they i) get past sunrise without erupting into a maelstrom of lawsuits and ii) get past "go-live" without imploding.

It runs contrary to industry standards where registrars whip their customer base into a frenzy over an exaggerated need to protect one's trademarks and claim one's stake in the latest "must have" TLD. The fact is, all you really need to care about are .COM, .NET and .ORG plus the ccTLD of the country you live in or do a lot of business in. (I will probably catch flack for saying .BIZ and .INFO are not crucial must-haves to your domain portfolio - we grabbed ours, at considerable expense in the case of .INFO and it was our experience in the roll out of these two that largely formed our policy.)

That most of these new TLDs roll out with initial 2-year registration period minimums are just an outright cash grab from the registry that most participating registrars are happy to join in on. They know that the sunrise and landrush frenzies they hope to whip up are the single greatest revenue events these TLDs ever experience. After the hoopla dies off and organizations realize how unimportant owning say ".ZX" is in their overall domain strategy and the domainers who piled in find out the aftermarket for the TLD is lackluster at best, the renewal rates predictably fall off a cliff.

So when the next "must have" TLD comes along and participating registrars start lovebombing their customers with reasons why they absolutely must "protect their name" in the new TLD, we often commit the egregious sin among investment bankers, VC's and pundits - that of "leaving money on the table" and we just don't rush in and push the new TLD. If it prevents us from leading our members off a cliff in to a major debacle, we consider ourselves as having done our job. (This was a similar rationale to why we never entered the IDN space, as long as you need a browser plug-in to make internationalized domain names even borderline usable they are, in our opinion, of marginal utility - we stayed out of it)

This is in line with our lifelong strategy of cultivating members who actually use their domains rather than pushing the "get your name before its gone" angle for every TLD under the sun on anybody who can fog a mirror. When we launched back in '98, we couldn't even register domains at all, so our member base was exclusively people who were actively using their domains and wanted outsourced DNS and/or forwarding. That set the tone for our positioning and culture ever since, and while now we do have a lot of customers using us "as registrar", our core is always the active domain users.

We have almost zero "domainers" with large portfolios of parked domains and speculative registrations because our model simply doesn't work for those types of users. It's not a judgement against domainers, it's just not where we came from.

All that said, you would probably think we are opposed to the new "free-for-all" TLD expansion policy hinted to in the recent ICANN meeting in Paris. We are not. We would welcome this new tlds policy (if it ever actually happens) because it removes the artificial scarcity and counteracts that "cashgrab" mentality we sniff at the root of many a new TLD. If new TLDs are coming out all over the place, two things happen:

- 1) Organizations realize that it is no longer practical to attempt to "protect their name" in every TLD space, so they stop trying. This removes a lot of the "easy money" underwriting new TLDs, some of which would otherwise launch for the thinly disguised reason of trying to milk the Sunrise for all its worth.
- 2) The above impetus gone, new TLDs will have to compete in a much more open market. Registries, while having de facto localized monopolies within their own TLDs will have to provide actual value to compete with other TLDs. That appeals to our sense of market freedom: less artificial barriers compelling a drive toward providing more value and benefits. The winners in the end should be the domain registrants, who are, let's not forget, our customers.

Posted by easyDNS: Domain Industry Watch in via easyDNS blog at 20:52

.ME Top Level Domain launch indicative of new TLD rollouts

We've gotten a few invitations to apply to be a .ME top-level domain registrar, to which we assigned no urgency after we took a straw poll internally and found that pretty well zero of our customers were asking for it. Today, Techcrunch reports that the .ME landrush, at least through one large operator, had degraded into a fracas. We have an unwritten policy here: new Top Level Domain roll outs are to be avoided until they i) get past sunrise without erupting into a

malestrom of lawsuits and ii) get past "go-live" without imploding.

It runs contrary to industry standards where registrars whip their customer base into a frenzy over an exaggerated need to protect one's trademarks and claim one's stake in the latest "must have" TLD. The fact is, all you really need to care about are .COM, .NET and .ORG plus the ccTLD of the country you live in or do a lot of business in. (I will probably catch flack for saying .BIZ and .INFO are not crucial must-haves to your domain portfolio - we grabbed ours, at considerable expense in the case of .INFO and it was our experience in the roll out of these two that largely formed our policy.)

That most of these new TLDs roll out with initial 2-year registration period minimums are just an outright cash grab from the registry that most participating registrars are happy to join in on. They know that the sunrise and landrush frenzies they hope to whip up are the single greatest revenue events these TLDs ever experience. After the hoopla dies off and organizations realize how unimportant owning say ".ZX" is in their overall domain strategy and the domainers who piled in find out the aftermarket for the TLD is lackluster at best, the renewal rates predictably fall off a cliff.

So when the next "must have" TLD comes along and participating registrars start lovebombing their customers with reasons why they absolutely must "protect their name" in the new TLD, we often commit the egregious sin among investment bankers, VC's and pundits - that of "leaving money on the table" and we just don't rush in and push the new TLD. If it prevents us from leading our members off a cliff in to a major debacle, we consider ourselves as having done our job. (This was a similar rationale to why we never entered the IDN space, as long as you need a browser plug-in to make internationalized domain names even borderline usable they are, in our opinion, of marginal utility - we stayed out of it)

This is in line with our lifelong strategy of cultivating members who actually use their domains rather than pushing the "get your name before its gone" angle for every TLD under the sun on anybody who can fog a mirror. When we launched back in '98, we couldn't even register domains at all, so our member base was exclusively people who were actively using their domains and wanted outsourced DNS and/or forwarding. That set the tone for our positioning and culture ever since, and while now we do have a lot of customers using us "as registrar", our core is always the active domain users.

We have almost zero "domainers" with large portfolios of parked domains and speculative registrations because our model simply doesn't work for those types of users. It's not a judgement against domainers, it's just not where we came from.

All that said, you would probably think we are opposed to the new "free-for-all" TLD expansion policy hinted to in the recent ICANN meeting in Paris. We are not. We would welcome this new tlds policy (if it ever actually happens) because it removes the artificial scarcity and counteracts that "cashgrab" mentality we sniff at the root of many a new TLD. If new TLDs are coming out all over the place, two things happen:

1) Organizations realize that it is no longer practical to attempt to "protect their name" in every TLD space, so they stop trying. This removes a lot of the "easy money" underwriting new TLDs, some of which would otherwise launch for the thinly disguised reason of trying to milk the Sunrise for all its worth.

2) The above impetus gone, new TLDs will have to compete in a much more open market. Registries, while having de facto localized monopolies within their own TLDs will have to provide actual value to compete with other TLDs.

That appeals to our sense of market freedom: less artificial barriers compelling a drive toward providing more value and benefits. The winners in the end should be the domain registrants, who are, let's not forget, our customers.

Posted by easyDNS: Domain Industry Watch in via easyDNS blog at 07:52

Blog Export: Exile From the Herd, <http://www.privateworld.com/>

Wednesday, March 26, 2008

Please note: ORDB anti-spam list no longer operational...

A number of our customers who maintain their own mailservers have called reporting issues with the delivery of their email in the last 24 hours. If you are experiencing something similar, please ensure that you are not using the ORDB anti-spam list.

The ORDB anti-spam list was shut down in December 2006, and in an effort to fully deactivate the list, ORDB is now sending out false positives. This means that if your mailserver relies on the ORDB anti-spam list, your mailserver is more than likely rejecting ALL EMAIL that is being relayed to it.

Please ensure you remove your mailserver's dependence on ORDB, as this will correct this specific issue.

Discussion about this recent development with ORDB can be found at the following URL upon

Slashdot:<http://it.slashdot.org/article.pl?sid=08/03/25/2124224>

Posted by easyDNS: Domain Industry Watch in via easyDNS blog at 14:46

Thursday, March 6, 2008

easyURL adds "FEDEX" tracking widget

Trivial but handy: I found myself having to email out some Fedex tracking ID's today, so I thought what would make it easy would be a way to create a redirect to the Fedex tracking page for that ID without having to visit a URL shortener site to create the redirect.

That's the core idea behind the "URL Widgets" or "Redirect Widgets" of easyURL, which are described here We also have them setup for Amazon products, domain lookups (surprise), Wikipedia pages and RFC's.

Posted by easyDNS: of Interest in via easyDNS blog at 15:08

Sunday, March 2, 2008

How to use your own domain name with Google Apps

Many Ayromlou does it again, publishing another step-by-step tutorial, complete with screen shots on how to use your own domain name on easyDNS with Google Apps..

Posted by easyDNS: Tips and Tricks in via easyDNS blog at 18:40

Tuesday, October 23, 2007

easyDNS announces Guaranteed Lookup Privacy for easyWHOiS.com

In light of the recent ICANN advisory on domain lookup frontrunning we've made the guarantee that your domain lookups on easyWhois have and always will be, private.

What is domain lookup front running? It is when an unscrupulous operator between you and a domain lookup tool, such as a whois lookup website, perhaps even the site operators themselves, monitor your domain name searches and then go and grab some of the available domain names you search on before you get the chance to.

I never thought anybody would be so brazen, but silly me, I once again underestimated the widespread use of sleazeball tactics on the internet.

You can read the easyDNS press release on the subject and our new Guaranteed Lookup Privacy Policy at easyWhois. We've also added SSL encryption to easyWHOiS to eliminate the possibility of queries being eavesdropped.

Posted by easyDNS: of Interest in via easyDNS blog at 15:45

Tuesday, September 11, 2007

Don't forget to vote in the CIRA Board elections

I just finished voting in the Canadian Internet Registration Authority Board of Directors election. This year's election is the first under the new election process and reformed membership structure that was ushered in last year at the special member's meeting in Toronto.

I have mixed feelings about the new membership reform, having spent a good deal of my term on the Board working on it and finally seeing it get ratified by the membership shortly after the end of my stint. I found the re-authorization process of the membership confusing. If I found it confusing, having been in the belly of the beast so to speak, it must have been utterly unfathomable to a lot of casual .CA domain holders. I think 90% of .CA domain holders don't even really understand who CIRA is or why they consistently get cryptic emails from them telling them to authorize this, confirm that, verify your id ("your paperssss pleasss").Continue reading "Don't forget to vote in the CIRA Board elections"

Posted by easyDNS: of Interest in via easyDNS blog at 10:52

Thursday, August 16, 2007

easyURL enables bookmarking and tagging with openid

You probably didn't know we operated a URL shortening service at easyURL.net, which has some nice features like being able to create your own short label for a shortened URL and tracking of access stats. After awhile I noticed that I was also using it as a pseudo-bookmarking mechanism, but of course it required that I actually remember the shortened URL. So we went ahead and added bookmarking and tagging to easyURL.net. The bookmarking features are accessible via OpenID tokens because we're finding people are getting less and less interested in creating a new account on every site they use. For people without OpenID, you can always use a site like del.icio.us, for those with, use this.

Posted by easyDNS: of Interest in via [easyDNS](#) blog at 14:00

Blog Export: Exile From the Herd, <http://www.privateworld.com/>

Thursday, May 31, 2007

How to use your domain name with blogger

Title says it all, easyDNS member Many Ayromlou wrote a clear step-by-step mini-howto today explaining the procedure to get your domain name registered through us working with your blogger.com blog:
<http://www.nerdlogger.com/2007/05/how-to-use-custom-dns-name-with-blogger.html>

My only comment is Step 6 shouldn't be a few hours' wait, not unless you've already typed your domain name into your browser before you do this and now your local ISP's nameservers have cached your old IP.

But thanks to Many, I'm sure a lot of bloggers interested on using their own domain name with blogger.com will reference this.

Posted by easyDNS: Tips and Tricks in via easyDNS blog at 20:52

Wednesday, December 6, 2006

Four essential components of Search Engine Optimization

I've been helping a longtime customer debug getting his website setup with a google sitemap and stealth redirection and he asked me in more general terms if I had any advice for him around search engine optimization. Here are four essential "must have's" for SEO. Three you can do right now, the fourth is not under your control as much. Before embarking on a concentrated SEO campaign, be sure the first three are in place. Continue reading "Four essential components of Search Engine Optimization"

Posted by easyDNS: Tips and Tricks in via easyDNS blog at 13:02

Monday, September 18, 2006

CIRA Board Elections On Now, Please Vote

During my 3-year tenure on the CIRA Board, I got the opportunity to travel across the country. Whenever we held a public forum anywhere in Canada, the turnout was usually quite high and the participants informed and enthusiastic. Then near the end of every open forum I made it a habit to ask the attendees the following question: "How many people here voted in the last election?" and the silence was usually deafening. Less than 10 hands would go up every time, guaranteed.

So why the disconnect between getting live bodies out to an actual event and getting stakeholders to click a few buttons through their web browser?

Given the discontent I've seen among netizens over some gTLD issues with .COM (remember sitefinder?) and ICANN oversight, CIRA has set the standard for accessibility and stakeholder guidance for .CA. People should be seizing these opportunities and making their views known and voting.

Running country code top level domain registries carry unique challenges and require industry experience balanced with a sense of stewardship. .CA is after all a "key public resource" and the kind of people I want on the Board are those that take that stewardship capacity seriously.

This year I'm voting for the following member nominees: Paul Andersen

[https://elections.cira.ca/2006/finalsplate/show/44/enClyde Beattie](https://elections.cira.ca/2006/finalsplate/show/44/enClyde%20Beattie) [https://elections.cira.ca/2006/finalsplate/show/22/enRoss Rader](https://elections.cira.ca/2006/finalsplate/show/22/enRoss%20Rader) <https://elections.cira.ca/2006/finalsplate/show/35/en>

And from nomination committee I'm voting for: Raymond Benoit [https://elections.cira.ca/2006/finalsplate/show/13/enBill Reid](https://elections.cira.ca/2006/finalsplate/show/13/enBill%20Reid) [https://elections.cira.ca/2006/finalsplate/show/12/enJeff Ryback](https://elections.cira.ca/2006/finalsplate/show/12/enJeff%20Ryback) <https://elections.cira.ca/2006/finalsplate/show/10/en>
I encourage all .CA domain holders who are CIRA members to vote now.

Posted by easyDNS: of Interest in via easyDNS blog at 16:11

Monday, July 10, 2006

Enhanced DNS resolution using OpenDNS

OpenDNS is an enhanced DNS resolver open to the public (as of today) and free to use. It contains a number of enhancements such as typo correction and phishing protection.

It is also fully configurable for the end users, so individual features can be turned off at the users' discretion.

I've also posted a comment on CircleID explaining why OpenDNS is not Sitefinder 2.0

(By way of quick explanation to the layman, there are three kinds of nameservers that affect your life: Root nameservers: which top level domain registries operate, such as the root nameservers for .com or .ca
Authoritative nameservers: for individual domains. This is the business easyDNS is in: answering DNS queries authoritatively for its member domains.
Recursive nameservers or resolvers: these nameservers find out DNS info on behalf of its users. Usually these are transparent to end-users and supplied by ISPs, often via DHCP. OpenDNS is now in this business.)

Posted by easyDNS: Domain Industry Watch in via easyDNS blog at 17:04

Tuesday, June 27, 2006

Want to reduce email spam to your mail server? Stop using backup spooling

It is with regret that we have come to the following conclusion, but here it is: Offsite backup SMTP spoolers and backup mail exchangers have become worse than useless

The problem is spam and the software that delivers it exploiting the weak authentication schemes inherent in the SMTP protocol itself. It used to be an annoyance, then it became a concern, it is now an epidemic and has resulted in the death of the offsite backup MX handler.

What happens is this: spammers try "dictionary attacks" on target domain names, trying to deliver email messages at random usernames at the target domain. The primary mailserver knows which usernames are valid and rejects the rest. The offsite backup MX spooler doesn't know what usernames are valid and what are junk, so it just forwards everything it receives for a domain it is spooling for to the primary MX handler.

Spammers and other malicious parties know this, so they may not even bother trying the primary MX at all, they'll just throw everything at the backup mail spooler which dutifully forwards it all (or tries to) to the primary. It is a dead-easy method of launching a Denial-Of-Service attack as well.

So it is with a heavy heart we have to admit that any utility of having an offsite backup MX handler is in most cases far outweighed by the advantages it hands to spammers and other miscreants.

The good news is this: without a backup mail spooler defined for your domain, originating mail servers simply queue the mail locally for a later retry. So owing to the design of the SMTP protocol, you do not really lose any redundancy when you remove a backup MX spooler from your DNS settings. But you probably cut down on the amount of spam your domain receives through the back door that is the backup MX spooler.

Posted by easyDNS: Tips and Tricks in via easyDNS blog at 16:33

Thursday, April 20, 2006

Seeking beta users for easySMTP: outbound mail service

We have been testing our outbound mail service (codenamed "easySMTP™") and it looks good. It supports TLS and listens on numerous alternative ports. easySMTP outbound mail service will be bundled with DNS-plus packages at no extra cost.

We are now accepting beta users for this service. If you would like to be a beta user and are currently subscribed with DNS-plus service, please contact support with your username and we will enable this feature for your account.

Many of us here at the office have been using this from home and it works great, so we anticipate a short beta period and a quick promotion to "production" status, at which point it will be available to all DNS-plus domains.

Details on the easySMTP outbound mail service can be viewed [here](#)

Posted by easyDNS: of Interest in via easyDNS blog at 11:41

Tuesday, February 28, 2006

China Top Level Domain news

There has been a remarkable lack of chatter today around domain policy circles, given the rather stunning announcement out of china that starting tomorrow, China will be launching its own Top Level Domain roots for the .COM, .NET TLDs so that "[Chinese] Internet users don't have to surf the Web via the servers under the management of the Internet Corporation for Assigned Names and Numbers (ICANN) of the United States."

Up until now, the underlying premise was that no matter what happened to naming policies, nothing would ever be done to change the tenet that (aside from deliberate design decisions like esoteric routing, geo-targetting, anycasting, etc) any two people typing "example.com" into their application could always expect the same results, forever.

Not so after tomorrow, when according to the one single article at the root of all this, China will be introducing .COM and .NET of their own.

CIRA Board member and internet governance commentator Michael Geist comments on the development here, and another domain insider I'll leave nameless (since it came in a private mail) said "Although innocuous you should mark and remember this day as the day the root was fractured - it is a big deal..."

I'm still trying to verify for myself that this is happening in the way it's been interpreted.

As I write this, it's approximately 2:45am March 1st in China and I'm not seeing any alternative root glue for .com or .net in the .cn root nameservers, which I was expecting to see. (It also begs the question: how will they backport a new root hints file into every single DNS resolver in the country?)

When I started this post, the soa on cn was

```
a.dns.cn. root.cnnic.cn. 2006022806 7200 3600 2419200 21600
```

and since I've been writing it has been changed to

```
a.dns.cn. root.cnnic.cn. 2006030101 7200 3600 2419200 21600
```

And also, since I've started this post, under the new SOA serial there are now these:

```
$ host -t soa com.cn
```

```
com.cn SOA a.dns.cn. root.cnnic.cn. 2006030101 7200 3600 2419200 21600
```

and

```
$ host -t soa net.cn
```

```
net.cn SOA a.dns.cn. root.cnnic.cn. 2006030101 7200 3600 2419200 21600
```

So I'm withholding reaction on this as I begin to suspect a poorly translated article was in reality announcing .com.cn and .net.cn subdomains which are non-events by comparison. Update:

It has become clearer after trading a couple emails around that the news is indeed that China has added com.cn and net.cn as well as their own alternate character set implementations for com and net.

Basically, this comes down to similar efforts over the years to launch competing or expanded root domains. What does make this interesting is that, while typically these enterprises are carried out by net.kooks, this is being done by a government. My guess is they will get some more traction than earlier efforts but what will eventually happen is ICANN (or whoever) will come to the table at some point and a way will be negotiated to maintain visibility and continuity in the root.

But for now, there is no fragmentation and no collision crisis to speak of. Update #2 (7:30pm EST):

Michael Geist just forwarded me this, the salient bit being:

The new domain name system also sets three temporary top-level domain names "China", "Company" and "Network".

This means from now on, the routing of these websites will go directly through the Chinese domestic analysis server instead of the ones used by ICANN. In effect, these three create an intranet within China.

This is tough to assess because I'm still unsure if this applies to the alternate character set com and net TLDs or if we're really talking about alternative com's and net's in China, which is pretty radical. This article re-iterates that the .com and .net TLDs are in the alternative chinese character set.

The excerpt above about the "domestic analysis server" makes me curious. Do they intend to somehow reroute requests inside China for the legacy .com and .net TLDs into the chinese charset ones? That would be extreme.

Another source whom I know likes to stay anonymous just emailed me:

Subject: sigh

I'm so surprised people didn't know China directs almost all root server requests to their own root?

They may not be taking over .com. but they have an alternate root for a while..

Still digging...(jeez, no pun intended)

Blog Export: Exile From the Herd, <http://www.privateworld.com/>

Posted by easyDNS: Domain Industry Watch in via easyDNS blog at 06:32

Monday, February 6, 2006

Yahoo and AOL's paid email delivery system

An interesting turn of events surfaced over the weekend with AOL and Yahoo's announced plans to charge a fraction of a cent for "preferred delivery" of email.

Both companies will still accept unpaid email, but by paying the charges, senders will be able to bypass inbound spam filters and have their mail delivered directly to the user's inbox.

The predictable backlash will come from this, but in terms of what we think about it here at easyDNS, we're ambivalent. We should go on record to our users now to state that we will not pay AOL or Yahoo on a per-email basis to get forwarded mail through. Mail passing through our forwarders will still be accepted by Yahoo and AOL, but if they add additional restrictions to it based on the fact that we haven't paid for preferred delivery, I foresee a mass exodus of email accounts from both services.

We are currently whitelisted by AOL, and I would even consider paying a monthly or annual license fee for that status based on our mail volumes, it would help us further differentiate as a premium domain manager and provide incentive to ramp up our spam filtering here (we're working on that as we speak). But the per-email delivery charge doesn't fit the model for mail forwarders and I see few, if any eager to assume those fees.

As mail forwarders, we're largely indifferent to where we forward our members' email to and our entire value proposition is based on the concept of giving our users the ability to route their email around network outages, localized ISP failures, and procedural and commercial roadblocks such as this.

Posted by easyDNS: Domain Industry Watch in via easyDNS blog at 08:34

MyPrivacy upgrades and new features

The MyPrivacy.ca whois-record-spamguard system has been upgraded to new hardware and now supports personalized whitelists.

This means individual users can add their own whitelists, either email based or hostname based, which opens myprivacy.ca up to much more flexibility beyond protecting your whois records.

An myprivacy.ca accounts are still free.

Posted by easyDNS: of Interest in via easyDNS blog at 08:31

Monday, November 28, 2005

Domain suffixes not an endangered species

I've seen several references to the firm that wants to get rid of net suffixes over the weekend, and at the risk of sounding like a stuffy curmudgeon I have to state my suspicion that it is at least partially attributable to a "slow technews weekend" after the US Thanksgiving. From monday morning's vantage point this outfit's 15 seconds of fame have probably already expired.

At first glance I thought this was another doomed protocol to sit on top of the DNS layer like the long defunct Realnames but further reading reveals this to be just another alternate root server initiative.

Whenever these things are brought to my attention I am quick to concede a few points: There is nothing revolutionary or innovative about creating an alternative root structure. All it takes is a nameserver. You can load anything you want into your root hints file and then try to convince people to use it. The current state of the DNS and the internet naming structure is built entirely on consensus and held together by convention. Thus, it is theoretically possible to alter consensus and change convention. There probably exist already "private" roots outside of the legacy namespace which are not visible to the world at large and this is intentional and by design (most VPNs can fit in the category but I suspect there are "pseudo-public" ones. My theoretical example has always posited the existence of a .CDC root for the Cult of the Dead Cow hacker group)

In practical terms, all you have to do is convince every nameserver operator in the world to change their root hints to [insert magic bullet solution to all the world's naming ills here] and if enough parties do it, absolute chaos will reign supreme until 100% uptake is achieved.

100% uptake will never be achieved. I have a friend who once made an apt analogy: "convince every car owner in the world to change their tires on the same day".

Thus, the best an alternative root structure can hope to achieve is to cause permanent and lasting damage, to in effect "break the internet".

If not enough parties do it, it will sink into the internet graveyard where all the other alternative root structures go to die. (It is a place that runs exclusively on IPv8 and INEGroup's Bindplus software has a de facto monopoly)

People may ask: Would easyDNS "support" these alternative roots? Our reply is that we'll provide DNS for anything our members want DNS for. If you want to give some company \$1000 USD to register "mycompany" as a Top Level Domain in a namespace nobody else on the planet can see, we'll provide DNS for it on request. It's your money. (We will caution you up front that this borders on vapourware) but to us it's just another zone in our nameservers (one that doesn't get a whole lot of queries).

Posted by easyDNS: Domain Industry Watch in via easyDNS blog at 10:01

Monday, September 19, 2005

Does your business advertise via PPC? Then stop paying for spammed clicks

One hears many complaints about Technorati's blog search engine, that all it does it return "useless" blogspam search results. Is this a sign of a "bad" search engine or is it indicative of a deeper problem within the blogosphere itself, that it's riddled with blogspam and automatically generated scraper sites? (Blogger is particularly bad because of its "export" feature. Spammers can export their entire blog to a remote server, thus scraper sites can distribute themselves over multiple IP addresses and keyword stuffed domain names and leverage the resulting linkpop into search engine results).

I've been noticing my technorati search for easyDNS almost always turns up more blog spam than anything else, i.e. <http://www.dnshostingpro.info/dns-hosting/dns+hosting.html>"Today's DNS Hosting Article" is a joke, it looks like the ad copy from ours and our competitors' Adwords campaigns being scraped out and simply concatenated into an keyword stuffed blob of crap with a Google Adsense block running over it. So those of us buying keywords via Google are paying for these ads on these scraper sites and something tells me those clicks are garbage traffic.

Last night I remembered that you can now click on the "Ads By Goooooogle" link in the corner of the Adsense block and report a policy violation, which I am now doing. I report that as a paying Adwords advertiser I'm not impressed seeing my keywords scraped and recycled into blogspam, only to pay for the priviledge of having my own ads run on them.

I think anybody buying Adwords should think about doing this. It only takes a minute: Subscribe to your own company name via Technorati's blog search and then complain about the blog spam you find scraping your ads. You'll be doing yourself and the blogosphere a service.

Posted by easyDNS: of Interest in via easyDNS blog at 11:45

Wednesday, July 6, 2005

Widespread PHP vulnerability in XML-RPC

I didn't bother mentioning the new PHP XML-RPC vulnerability to somebody yesterday, assuming they already knew. Alas, they got burned by it so I'm making it a point to mention these things in a widespread generic sense from now on. As such: if you are running PHP content management systems like blogs, postnuke or anything that uses PEAR XML_RPC

Posted by easyDNS: of Interest in via easyDNS blog at 14:58

Friday, June 3, 2005

Domain name dispute in Canadian House of Commons

It'll be interesting to see what comes of the domain name dispute debate which took place in the House of Commons over same-sex marriage opponents who registered MP's names as domains and setup websites on them to drum up support for their cause. As Michael Geist comments, the actions are nebulous and under the current rules in place at CIRA, these do not constitute "bad faith" registrations and thus not really eligible for action under the CDRP. I don't expect this to be added to the agenda for next week's CIRA Board meeting in St. John's Newfoundland (my last one as a director), but we may get a few questions on it during the public forum. What eludes me in this day and age is how semi-public figures like politicians don't bother registering their own names as domain names as a matter of course. At the very least they can avoid situations like this and at best the clueful (and bold) ones can run blogs on their own domain names. Note: I later found out that this domain was registered and then allowed to lapse, where it subsequently washed out via TBR and was picked up by the current registrant. While there are, I am sure, other members of the politburo who have not adequately guarded their own named domains, this illustrates another point, that of formulating a coherent domain registration and retention policy within your organization, as described in our Domain Management Resources: 10 Domain Management Tips article.

Posted by easyDNS: Domain Industry Watch in via easyDNS blog at 13:07

Thursday, May 19, 2005

Canadian Anti-Spam Task Force report

Yesterday Industry Canada's Anti-Spam Task Force delivered its report. Included therein was a group of industry best practices assembled by the Working Group on Network Technology sub-group which I was privileged to take part in. This analysis is posted on CircleID while Michael Giest, who was on the Task Force and chaired the Legal Issues Working Group, discusses next steps at his webpage. In a nutshell, the ISP Best Practices are as follows:

1. All Canadian registrants and hosts of domain names should publish Sender Policy Framework (SPF) information in their respective domain name server zone files as soon as possible. [Follow this link if you are interested in implementing SPF on your domains at easyDNS]
2. ISPs and other network operators should limit, by default, the use of port 25 by end-users. If necessary, the ability to send or receive mail over port 25 should be restricted to hosts on the provider's network. Use of port 25 by end-users should be permitted on an as-needed basis, or as set out in the provider's end-user agreement / terms of service.
3. ISPs and other network operators should block email file attachments with specific extensions known to carry infections, or should filter email file attachments based on content properties.
4. ISPs and other network operators should actively monitor the volume of inbound and outbound email traffic to determine unusual network activity and the source of such activity, and should respond appropriately.
5. ISPs and other network operators should establish and consistently maintain effective and timely processes to allow compromised network elements to be managed and eliminated as sources of spam.
6. ISPs and other network operators should establish appropriate intercompany processes for reacting to other network operators' incident reports.
7. ISPs, other network operators and enterprise email providers should communicate their security policies and procedures to their subscribers.
8. ISPs and other network operators should implement email validation on all their Simple Mail Transfer Protocol (SMTP) servers (inbound, outbound and relay).
9. Non-delivery notices (NDNs) should only be sent for legitimate emails.
10. ISPs and other network operators should ensure that all domain names, Domain Name System (DNS) records and applicable Internet protocol (IP) address registration records (e.g. WHOIS, Shared WHOIS Project [SWIP] or referral WHOIS [RWHOIS]) are responsibly maintained with correct, complete and current information. This information should include points of contact for roles responsible for resolving abuse issues including, but not limited to, postal address, phone number and email address.
11. ISPs and other network operators should ensure that all their publicly routable and Internet-visible IP addresses have appropriate and up-to-date forward and reverse DNS records and WHOIS and SWIP entries. All local area network (LAN) operators should be compliant with Request for Comments (RFCs) 1918 "Address Allocation for Private Internets." In particular, LANs should not use IP space globally registered to someone else, or IP space not registered to anyone, as private IP space.
12. ISPs and other network operators should prohibit the sending of email that contains deceptive or forged headers. Header-tracing information should be correct and compliant with relevant RFCs, including RFC 822 and RFC 2822, and reference domains and IP addresses should have up-to-date, accurate registration information.

I'll follow up in a later post on my personal thoughts on these recommendations but I will mention here that I'm very happy to see #9. The amount of backscatter clogging up the net from broken spam and virus blockers is just compounding the problem and helping absolutely nobody.

Posted by easyDNS: Domain Industry Watch in via easyDNS blog at 17:53