CircleID
INTERNET INFRASTRUCTURE

This is the Print View Page

« Back to Full View

Taking Back the DNS

Jul 30, 2010 10:04 AM PDT | Comments: 154 | Views: 155,388

By **Paul Vixie**

Most new domain names are malicious.

I am stunned by the simplicity and truth of that observation. Every day lots of new names are added to the global DNS, and most of them belong to scammers, spammers, e-criminals, and speculators. The DNS industry has a lot of highly capable and competitive registrars and registries who have made it possible to reserve or create a new name in just seconds, and to create millions of them per day. Domains are cheap, domains are plentiful, and as a result most of them are dreck or worse.

Society's bottom feeders have always found ways to use public infrastructure to their own advantage, and the Internet has done what it always does which is to accelerate such misuse and enable it to scale in ways no one could have imagined just a few years ago. Just as organized crime has always required access to the world's money supply and banking system, so it is that organized e-crime now requires access to the Internet's resource allocation systems. They are using our own tools against us, while we're all competing to see which one of us can make our tools most useful.

My thinking when I created the first RBL (now called a DNSBL; mine was the MAPS RBL though and so that's how I still think of it) back in the mid/late 1990's, was that universal access between e-mail servers was a greater boon to the bad guys than to the good guys, and so I worked to create a way that cooperating good guys could make their mailers less accessible. While I didn't reach my objective of stopping spam, I did help establish the "my network, my rules" theory of limited cooperation for Internet resources. Simply put, it's up to every network owner to decide who they will or won't cooperate with, and the way to get your traffic accepted by others is to be polite and to spend some effort trying to avoid annoying folks or letting your customers annoy folks.

Here, in 2010, I've finally concluded that we have to do the same in DNS. I am just not comfortable having my own resources used against me simply because I have no way to differentiate my service levels based on my estimate of the reputation of a domain or a domain registrant. So, we at

ISC have devised a technology called Response Policy Zones (DNS RPZ) that allows cooperating good guys to provide and consume reputation information about domain names. The subscribing agent in this case is a recursive DNS server, whereas in the original RBL it was an e-mail (SMTP) server. But, the basic idea is otherwise the same. If your recursive DNS server has a policy rule which forbids certain domain names from being resolvable, then they will not resolve. And, it's possible to either create and maintain these rules locally, or, import them from a reputation provider.

ISC is not in the business of identifying good domains or bad domains. We will not be publishing any reputation data. But, we do publish technical information about protocols and formats, and we do publish source code. So our role in DNS RPZ will be to define "the spec" whereby cooperating producers and consumers can exchange reputation data, and to publish a version of BIND that can subscribe to such reputation data feeds. This means we will create a market for DNS reputation but we will not participate directly in that market.

The first public announcement of DNS RPZ was at Black Hat on 29-July-2010 and then at Def Con on 30-July-2010.

The current draft of "the spec" is here. No backward-incompatible changes are expected, and both reputation providers and recursive DNS vendors are encouraged to consider developing products that use this format to express DNS reputations.

The current patches for BIND9 are shown below. We expect this functionality to be part BIND9 9.7.3 which is several months off. Customers of ISC's BIND support should contact ISC before applying these patches or any other patches to their production systems.

- BIND9 9.4-ESV-R2 patch
- BIND9 9.6-ESV-R1 patch
- BIND9 9.7.1-P2 patch

Comments and questions can be sent here. I'd especially like to hear from content providers who want to be listed by ISC as having reputation content available in this format, and also recursive DNS vendors whose platforms can subscribe to reputation feeds in this format. An online registry will follow.

We're about to enter a bold new world where the good guys do not automatically grant the use of their DNS resources to bad guys. I don't like the need for this but I'm finally pulling my head out of the sand. So, let's party.

By Paul Vixie, CEO, Farsight Security. Visit the blog maintained by Paul Vixie here.

Related topics: Cybercrime, Cybersecurity, DNS, Domain Names, Registry Services