ICANN Start, Episode 1: Redirection and Wildcarding

Recorded in October, 2009

[Music Intro]

Welcome to ICANN Start. This is the show about one issue, five questions:

- What is it?
- Why does it matter?
- Who does it affect?
- Who's going to fix it?
- What can I do about it?

Produced by the Policy Team at the Internet Corporation for Assigned Names and Numbers.
ICANN. One world. One Internet. Everybody connected.

Scott: Thanks for joining us on the first official episode of Start. I'm Scott Pinzon. Our topic for this episode is redirection -- more specifically, we're talking about redirection at the top level of the Domain Name System, a practice also sometimes called "synthesized response" or "wildcarding." Our subject matter expert is Dave Piscitello, Senior Security Technologist for ICANN and a popular member of ICANN's Security and Stability Advisory Committee.

I caught up with Dave at the Lotte Hotel in Seoul, South Korea. Here's what he had to say about redirection -- beginning with our first question: What is it?

Dave: The most important thing for us to do at the outset is just to set the context of how the DNS works. So we're going to have a small DNS 101.

Scott: Oh, I think listeners would appreciate that.

Dave: Most people are familiar with the fact that the Domain Name System is often used to determine the IP address associated with the domain name. So there's a number, and what we want to do is essentially find that number when we make a query to the DNS on a name like example.com. This is called domain name resolution.

Scott: So, this is how instead of having to remember the IP address of Google or Amazon or something, I can type Amazon.com and it will resolve to whatever IP address that is.

Dave: Exactly. Now under normal circumstances, the DNS responds to a query in one of two ways. If the name is found in what's called the "zone file" (which is essentially the database of names for a particular registry. A registry is something like dot-com or dot-net or dot-org, or one of the country code TLDs.) -- so, if the name is found in one of those zones, a positive response containing the IP address associated with that name is returned to the querying party, the user. If a name is not found or is a special error called "non-existent domain," that's returned in the response. You all clear?

Scott: Yeah, and most of the time, the typical user is working this out through their web browser, right?

Dave: Exactly.

Scott: I typed a URL and I've hit "go", that's actually a query to the DNS.

Dave: Yes. It ends up in a query to the DNS. So, redirection actually alters this fundamental behavior in the following way. You only get positive responses from the DNS. There are two kinds of positive responses. The first kind is exactly what I described before. If the name is found in the zone file, you will get the IP address associated with the name.

The second type is a synthesized response. In a synthesized response, instead of receiving a "non-existent domain" error, the response message contains a signal indicating there was no error. And it returns an IP address that the zone authority, the operator of the name server, chooses.

So, instead of getting a response that says, "I can't find example.com," it says, "I found example.com and here is the address I've chosen to assign to it."

Scott: I think I get the concept but let's follow up a little more with your example.com to clarify.

Dave: Sure. Suppose I type ww.example.com –

Scott: Instead of www?

Dave: Right. My finger slipped, and this is fairly common.

Scott: Sure.

Dave: I hit the Enter key and I should get an error message because this is not really a name that example.com intentionally placed in its own file.

Scott: Yeah, they didn't make ww.example.

Dave: Right. So, because ww.example doesn't exist in example's zone file, someone decides, "I'm going to return an IP address." That IP address takes me to a search page as opposed to the webpage, www.example.com.

Scott: Oh, I see.

Dave: So, as a consequence of my mistype, instead of going to the web page I wanted to visit, I'm now directed, or in fact, **re**directed to a search page that a zone operator chose to direct me to. That page could have pay-per-click advertising. It could have a different search engine than the one I normally use. And it might even install malware.

Scott: That is starting to foreshadow our next question. We now know what redirection is. Next question is, Why is this important? But I think I'll phrase it this way: Why would anyone do redirection and why would anyone be opposed to redirection?

Dave: So, let's look at the marketing or positive benefits that are associated with redirection.

Scott: Okay.

Dave: One argument is that Internet users don't benefit from receiving errors, but they benefit from an error being resolved to some page that provides them with a solution to the problem.

Scott: I see. So the thought is, "I don't have your true answer but I'm helping you along the way."

Dave: Exactly. So, for example, you could go to a redirection page and it says, "You were trying to get to ww.example.com. Perhaps you meant to go to www.example.com." In the meantime what they've done is they've placed pay-per-click advertising on that site that says, "Oh, you could also be visiting example.2.com and get much the same information."

Now, if you click the pay-per-click, what you've ended up doing is providing the one who's hosting the redirection page with a value-add, because they're making money off redirecting you further to another page.

The monetizing traffic in the form of pay-per-click or in the form of payments that a search engine will offer you by the fact that you're hosting their search engine on your page, are two reasons why people would do a resolution.

Scott: So, it's actually a part of some people's revenue model.

Dave: A very big part, in some cases.

Scott: Then there's another camp that's opposed to redirection. Why would that be?

Dave: There are actually two important aspects to understanding the problems that can arise with redirection. One is that thus far we've only talked about the Internet as if the only application is web. But imagine if I'm doing this with mail, or imagine if I'm doing this with a voice call, using voice-over-IP. A little bit different, isn't it?

Scott: Yeah, it is.

Dave: A second and very important factor is that suppressing those errors fundamentally changes the way the DNS protocol works and that breaks things.

Scott: What kinds of things does redirection break?

Dave: I think many of our listeners are probably familiar with network management applications or utilities, such as "ping." Ping is a program that you use to test to see if a host is alive and present on the Internet and say, "Ping" and domain name, or "Ping" and an IP address. If you get a response you know that the host is up.

Scott: Right.

Dave: Well, suppose you only get positive responses every time you ping.

Scott: Whether the host is up or not.

Dave: That means that you never know whether the host has gone down.

Scott: Because you did a ping but it got redirected to something that's responding.

Dave: Exactly. The same is true for things like traceroutes. The same is true for many applications that rely on the ability to distinguish when a host is up, when a name resolves and when a host is down where the name is not resolving. Even domain name system administrators, folks who run name servers need to be able to understand when their name server is up and down.

Scott: This is like removing one of your five senses. You're trying, as a network administrator, to know what's going on. Now you've kind of lost the ability to sense when certain things are down.

Dave: Right. Now, let's look at some other things that might give people a little bit more nervousness. Imagine our email systems and redirecting traffic that's supposed to go to an email system that's run by your company to a host that is either not hosting a mail service or a host that's hosting mail service that's not your mail service.

Both those scenarios result in essentially a denial of service of mail delivery. In the worst case, somebody that you don't want receiving your mail is actually spooling all your mail on their machine.

Scott: And since mail is almost always clear text, there goes all your privacy. There's all kinds of trouble they could cause.

Dave: Exactly. In fact, hijacking emails and trying to hijack email servers is something that has been a traditional attack factor.

Scott: It sounds like you're saying that generally any kind of application that uses a client and a server needs some way to distinguish between success and error.

Dave: There are thousands of applications. Folks who are in favor of redirection probably haven't investigated the consequences for all of them.

Scott: We've talked about what it is. We now know why it's important. So our next question is who should care about this or who does this affect?

Dave: Just about everyone.

Scott: Okay. Maybe you could put some detail behind that.

Dave: Well, so, web users in both a positive and negative sense are trying to recognize the folks who do believe in error resolution. Network administrators are affected adversely as we just talked about. We talked about email users and operators. We didn't really talk about voice-over-IP users. But imagine that a redirection is performed on a voicemail server.

Scott: Wow.

Dave: That's going to redirect me away from my voice mailbox and to some other location. Now we've only talked so far about benign redirection. We haven't really talked about malicious redirection.

Scott: That was something that was occurring to me in the background, is that you cannot assume that the person doing the redirecting has your interests in mind.

Dave: We could probably do an entirely new and additional segment on just what happens when you have malicious redirection. For now, understand that more voicemail systems require

PINs. And if I go to a maliciously-hosted voicemail server and I submit my PIN, I've now disclosed my PIN to someone who shouldn't really be receiving it.

Scott: All right. So, we put some detail behind the idea that redirection and synthesized responses could affect almost every Internet user. So, let's move on to our fourth question, who's supposed to fix this issue?

Dave: Redirection can be performed at many levels of the DNS. But ICANN can only influence the policies and practices at the top level of the DNS or the Generic Top-level Domain Registries.

Scott: Right. What we often call gTLDs.

Dave: The Board of Directors at ICANN has considered the matter and determined that redirection should be prohibited in all new applications for generic TLDs.

Scott: The generic top-level domains are not here as we're recording this, but they're working through the process where people can apply to own and operate a new TLD. That process is outlined in a Draft Applicant Guidebook. Somehow we shortened that to DAG. Does the DAG address this?

Dave: The DAG does address this. There is also an explanatory memorandum, or malicious conduct in new gTLDs. That memorandum explains in more detail why redirection is not desirable and why the Board has recommended that it be prohibited.

Scott: If it's already prohibited in the TLDs to come, what is there left to do, if a listener cares about this issue?

Dave: Remember we said "**draft** applicant guidebook"?

Scott: Okay.

Dave: ICANN is a multi-stakeholder consensus policy process. It's very important for the community to either embrace or oppose policy that is going to be imposed upon future generic top-level domain registries.

Scott: The Draft Applicant Guidebook will be going out in another version for public comment. There's an opportunity there to weigh in for or against redirection.

Dave: Yes, and expressing support or opposition during these public comment periods is important. And in fact, there are currently public comment periods for not only the Draft Applicant Guidebook, but for the explanatory memorandum on what's called "malicious conduct."

There's also a public comment period for what's called a High-Security Zone Verification Program. They're very easy to get to. What you can do is start by clicking on the new top-level domains icon on the ICANN home site, and drill down from there.

Scott: If you go to ICANN.org, there's a nice little button over on the left for new gTLDS. They put together a great page with a lot of resources. So, hit that and start looking for the links and you can find all these resources.

Dave, thank you very much for a careful and very clear description of redirection. There's actually a lot more to it than you might first think when you see the term.

Dave: That’s very true, Scott. Today we’ve only had time to talk about well-intentioned applications of redirection. If you are interested in reading more about some of the potential malicious activities and some of the unintended consequences of redirection, the SSAC has published a report, Document Number 32, called DNS Response Modification. That’s available at the SSAC web site.

Scott: So, to navigate there you would just go to ICANN.org and then look for information related to the Security and Stability Advisory Committee, or SSAC. Or you could just search on SAC 032.

Dave: Both would work.

Scott: And, I’m going to recommend another one. SAC 41 is the recommendation that prohibits use of redirection and synthesized responses. Might be worth a person’s time also.

Dave: That’s true.

Scott: All right. Well, dear listener, you’ve got plenty of work cut out for you, if you’d like to learn more about redirection. Thanks for listening and join us again next time.

[Music]

What do you think of this podcast? We’re eager to find out. Email your comments, questions and ideas for topics to Start@ICANN.org.

IC ANN – One world. One Internet. Everyone connected.