***ICANN Start,* Episode 9: Protecting Your Domain (SAC044)**

Released 23 February, 2011

[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 Internet Corporation for Assigned Names and Numbers, ICANN: One world. One Internet. Everybody connected.

Scott Pinzon: Yes, this is *ICANN Start*. I'm Scott Pinzon and after a hiatus we are back by popular demand. Thank you for your many kind comments and we expect once again to have a new episode for you at the start of each month.

To re-launch our podcast we continue as we first began by chatting with the Senior Security Technologist of ICANN's Security and Stability Advisory Committee, known for short as SSAC. Our first ever episode featured this man, and I'm proud to welcome back Dave Piscitello. How are you, Dave?

Dave Piscitello: I'm fine. Thank you, Scott.

Scott Pinzon: Thanks for being with us this episode. SSAC has just issued a significant report known for short as SAC044, but I gather it's about how to protect your domain registration accounts and domain names against attacks and misuse. Can you give us a little more idea of what SAC044 is?

Dave Piscitello: Yes, Scott, I'd be happy to. SAC 044 is a guidebook. It's actually quite an exhaustive guide, and it discusses how individual domain name registrants -- folks who register domains, and even large organizations, and everyone in between – can implement measures themselves, protect themselves against account compromise or the accounts that they hold at domain name registrars, for example. And also against attacks that can be executed by an attacker once an account has been compromised.

Scott Pinzon: So when you're talking about account compromises, is that kind of techie-speak for, "They took my domain name from me"?

Dave Piscitello: No, I'm actually talking about someone essentially hacking your account, just like they would hack your bank account. They break into the web portal that a registrar provides you to manage your domain names; or they steal your credentials and they impersonate you with a registrar's staff and somehow manage to gain hold of the account.

Once they gain hold of the account, of course, they are able to control and administer the domain names in that account portfolio. So if you hold example.com and example.org and example1.com and on and on, then not only will the attacker have access to your account but he also has access to changing the contact information of your account, changing the email addresses where notifications are sent, and even changing the DNS configuration – how your names resolve.

And so that's a particularly valuable vector for an attacker because what he can do is he can redirect anything that's going to your web to a site that he's hosting at an IP address that he's controlling.

Scott Pinzon: Okay, now you've got me good and scared. All that sounds awful. Can you give us some examples of what SAC 044 describes that would help prevent those things from happening?

Dave Piscitello: Well, SAC 044 is prescriptive in a number of ways, and we tried to include and consider someone as simple as a micro-business or a home operator as well as someone who has a full scale IT department and other staff that are managing a large portfolio of domains. Some of the remedies and the prescriptive measures that we describe are as simple as keeping track of your accounts, keeping track of the registrar's points of contact – people that you would reach out for in the event that you had someone hijack your account.

Some of the other measures are also simple: using good, basic password management and composition. Others have to do with what I've referred to in the past, being a South Carolinian and being in the Hurricane Belt, as a "hurricane box" – a set of documentation that you maintain for yourself and you carry with you in the event that you're evacuated. And all that documentation does is essentially allow you to create a restore point, so to

speak, if you suffer some sort of damage or your property suffers some sort of damage in a hurricane.

So the documentation that we're thinking about here is proof that you have the registration that you claim to have in the form of correspondence from a registrar, a Whois print out of the domain that demonstrates that you are the contact owner at a particular point in time prior to the attack. Those are the simple measures.

The more complex measures get to the point where we talk about things that larger enterprises could do that are very similar to some of the features and services that some of what we call "online brand protection companies" do. These involve things like monitoring your DNS very proactively to see if there's any changes and then making certain that the changes were changes you authorized; or monitoring your Whois to make sure that nobody's gone and monkeyed with your Whois and altered the contact information.

Scott Pinzon: Now a lot of the folks who listen to *ICANN Start* would probably fall in the category of an individual domain holder or what we might call a micro-business or a small business. I understand why the measures you're describing would help but they seem like a lot of work for an individual to go through.

Dave Piscitello: Right, and we considered that. And in fact, one of the reasons why we opted to try to make this rather an exhaustive document is to provide enough information where folks who would actually appreciate the value of their domain and how important it is to keep it and renew it, and what problems they would have maintaining their online presence, would be able to use the document as a learning tool and then also use it as criteria for selecting someone to manage this on their behalf.

So they could go to their Internet service provider, they could go to a registrar, they could go to an online brand protection company and say, "I'd like you to now manage my accounts, and I'd like you to manage my domain name portfolio. And here are the things that I've learned about that I really want to make certain *you* are able to provide for me."

Scott Pinzon: Okay, that could provide some relief. It's not all down to one person all by themselves.

Well, part of our tradition here after we ask "What is the issue?" is then to ask "Why does it matter?" And I think I can see that, but would you please address that for us? Why does this issue matter?

Dave Piscitello: Let me put on a security professional hat for a minute and talk about assets and risk. If you have a domain name and you're an eBay or a Go Daddy or any of the large companies, and that domain name is not resolving, that's a very, very significant business impact on the order of millions of dollars for certain merchants per minute.

If you are a small, individual domain holder you may actually exact the same sort of financial loss, but possibly over a long period of time. Someone who is an individual domain holder might not get the number of hits that Amazon does, but if you're missing visitors for an hour or a day or a week, and you're not aware of it, you're missing revenue.

Scott Pinzon: Yes, and it's all relative. It may not be millions of dollars but it might be what your family depends upon to pay its bills. So in a felt sense it's just as much.

Dave Piscitello: Right. And revenue is only one aspect of paying attention to risk. It's also reputational harm. If someone takes your domain and they use it for a phishing attack, or someone uses it in some way to deface your site or embarrass you, those sorts of incidents are the kinds of things that essentially render your domain very, very less valuable than it was to you before the incident.

Scott Pinzon: Dave, I'm sitting here picturing the listener hearing all this, and I'm going "You know what? I don't really have any enemies, and most people don't know about my account. I don't think anybody's going to come after me. And I think probably my registrar protects my account anyway." Is this a realistic attack for most people?

Dave Piscitello: Yes, because a lot of the domain attacks are attacks of opportunity. And in fact, we have seen many circumstances where perfectly benign and off-the-radar domain names end up being compromised because phishers will go out and they will actually impersonate a registrar and send correspondence to domain holders and say, "Oh, there's a problem with your account. Could you please log in and fix this?"

Well, some people panic, other people read it and it looks very credible. And they go and they log in, and then their account is stolen just as it would be in any other phishing attack.

Now, the value of that domain to a phisher is pretty obvious – it's a legitimate domain. It's not a brand new registered domain that is immediately earmarked by the security community as a malicious registration. So the security community has to tread a little bit differently, and registrars have to tread a little bit differently when they go and they try to investigate that domain. They don't take it down as quickly because the evidence is not so obvious.

Now you also asked, Don't the registrars protect your account? Well, registrars do but remember that registrars use the same applications and security products and techniques that e-merchants and financial institutions and other security-savvy companies do. We all know from what we see every day in the security news that there are exploits that are used against all these kinds of web presences to compromise web-based accounts.

Then there's also that really, really nasty social engineering aspect that I talked about earlier – the phishing attack, the email that lures you into doing something you really should not. So while the registrars do provide protective measures, this is one of those "physician heal thyself" kinds of positions. You can rely on someone else to do it all for you or you could also try to do some of it yourself.

In the security world, as you and I know from our history in working with firewall companies, there's this notion of defense in depth. So you can actually think of SAC 044 as being a way for you to understand what the registrar can provide for you or a third party domain name account manager, and what you can provide for yourself. And sometimes duplication is good because sometimes duplication provides you with that sort of defense in depth.

Scott Pinzon: All right. So in some ways you've anticipate the next question, which is "Who does it affect?" But if you're saying that oftentimes these attacks happen because there's an opportunity, the attackers see a weakness, I guess you could say that everyone with a domain name should be concerned. Is that right?

Dave Piscitello: Yes. And the qualifier here is, the extent to which you should be concerned is sort of directly related to the value you ascribe to your domain. And eBay or

an Amazon or a Google are going to spend a considerably more amount of money than some mom & pop embroidery shop. And I'm not saying that the domain is not necessarily important, but the emphasis on how much effort you put in has to do with risk and benefit. So the risk/benefit analysis or the cost/benefit analysis is going to be different for the individual versus the enterprise.

Scott Pinzon: So you don't spend $10 of security to protect $1 of domain value. Is that kind of the message?

Dave Piscitello: That's right. Exactly. So there's a percentage of the amount of money you would want to invest in protecting an asset that every organization, and even an individual, decides. It's very similar to insurance – not everyone wants to go out and buy a $20 million life insurance policy because the cost of that is exorbitant. Some people want at least $10,000 or $20,000. So what's the cost and what's the reward?

Scott Pinzon: Yeah, I see. Dave, you mentioned earlier the idea of choosing partners that could help you. You mentioned online brand protection companies. I don't even know how to look up online brand protection companies. I doubt that's in the phone book, so how do you select partners if you want help protecting your accounts?

Dave Piscitello: Well, there are a couple of different ways you can do this, and obviously search engines are very valuable. And in fact, if you type "online brand protection" you get quite a few very competent companies.

But for example, we're talking about two features and services that registrars commonly provide – a registration service and then a service that they normally use to host and resolve your domain names through IP addresses. Some of those are actually provided by what are called resellers, and resellers can be ISPs or they can be web hosting companies, or they can be provided by registrars. And there's a long list of companies that do this.

The online brand protection companies tend to be more of the higher price spread, so to speak; therefore the companies who are in the Fortune 1000, who really, really need to make certain that not only their domains resolve but there is no one running around, treading on their intellectual property and trademarks. So those managed companies and providers are the kinds of trusted partners you see in enterprises.

But even if you're just going to choose among registrars, it's certainly valuable to go and look at all the registrars who are offering what appear to be the same services, and then look a little bit under the hood. What are they actually implementing and what are they actually doing? And what services do they offer that seem to correspond to what SAC 044 recommends that are appropriate for your niche – individual, micro-business, medium business, enterprise?

Scott Pinzon: All right, Dave. So far you've given us a nice brief description of the issue itself and things we can do to defend our accounts. Am I correct in assuming that in SAC 044 there's much more detail along these lines?

Dave Piscitello: Yeah, extensive detail. And we've tried very hard to use relatively plain language – obviously security is not always plain language. But for example, we tried to explain to people what they have to protect themselves against, and we outlined the sets of attacks or the sets of exploits that someone can try to use to compromise your account and to gain access to your domains.

We then talk about a litany of things. We talk about how to protect your contact information in your registration record, how to protect and monitor your domain name service; how to treat routine correspondence from your registrars and use those as almost like part of a workflow for an organization. So you get a notification of a renewal, you get a notification of a change in a large organization and what you might do is say "Ah! I have to immediately get the people who are responsible for domain names to pay attention to this." So it's almost like a little alert, like a pop-up on your desk that says time to go to a meeting.

And those are good things for large-scale enterprises. We also talk about the kinds of measures that you can use to monitor, and how you monitor, your registration contact information by using Whois and automating it rather simply to just go out and check Whois on a regular basis and make certain that nothing's been altered. You can do the same thing with your domain name service.

So we go into some detail about each and every one of those things. Then we try to do something that I think is fairly valuable for almost anyone. At the very end of the document we have two sections that talk about the kinds of questions that you should ask of anyone that you're going to choose as your partner in managing your domains or your DNS, so that you can make an

informed decision as to whether this is the best party that you want to partner with.

And there's one set of questions for registrars, and there's one set of questions for registries. These questions are really designed to answer the question "How do I choose?"

[Music]

Scott Pinzon: That sounds terrific. So if you're listening to this and you realize "Well, I have a domain registration account and I haven't really covered all these issues," I really encourage you to read SAC 044. And it's not hard to find – you can go to SSAC's website, which is www.ssac.icann.org, and as soon as you go there on the left nav you'll see a little choice that's "SSAC Documents." And you can look for SAC 044 there.

Dave, thank you for bringing us a report on your report. I'm really glad you brought it to our attention.

Dave Piscitello: Thanks for giving us this opportunity. I hope people will go and read and think carefully, and study up. The best thing that you can do to make the whole net more secure is make an informed choice.

Scott Pinzon: Thank you, Dave.

[Music]

Now that you've enjoyed the first 2011 episode of *ICANN Start*, be sure to watch for our March episode, when I'll interview Olivier Crepin-Leblond, the new Chair of the At-Large Advisory Committee. Olivier discusses his own history with ICANN, what makes At-Large the voice of the individual Internet user, and what they mean by "ALAC 3.0." Join us next time, on *ICANN Start*.

[Music]

ICANN Start is an educational service from the Internet Corporation for Assigned Names and Numbers: ICANN. One world. One Internet.

[End of Transcript]