Domain Name Server (DNS) Blocking

featuring Vijay Sarvepalli as Interviewed by Suzanne Miller

Suzanne Miller: Welcome to the SEI Podcast Series, a production of Carnegie Mellon University Software Engineering Institute. The SEI is a federally funded research and development center, operated by Carnegie Mellon University and sponsored by the U.S. Department of Defense. A copy of today's podcast is available on the SEI website at www.sei.cmu.edu/podcasts.

My name is Suzanne Miller. I am a principal researcher here at the SEI. Today, I am very pleased to introduce my colleague, Vijay Sarvepalli, who will be speaking to us today about DNS, Domain Name Server Blocking, as a strategy for combatting cybersecurity threats.

So, I want to welcome Vijay. And before we get started into the topic itself, our viewers want to know a little bit about who are you and what brought you to the SEI to do this kind of work? What is it that makes this work important to you?

Vijay Sarvepalli: As you introduced, I work at the SEI at the CERT Division, which is actually the cybersecurity division. I come from a background of electrical and computer engineering, over 25 plus years of working in different electric and computer problems. Our division is focused on basically building responses to cybersecurity threats, both with the technology process and with the training and different tools we provide. My specific role is to help very large enterprises, like the government and the DoD, deal with cybersecurity and build security solutions for it.

Suzanne: So, you are looking at it from an enterprise systems viewpoint.

Vijay: Yes, absolutely, very large-scale systems, very high impact, really targeting to support somebody like a CISO or vice-president of security, to…

Suzanne: So, a CISO is a…

Vijay: Chief Information Security Officer.

Suzanne: Information Security Officer. I keep saying CSO, but I am seeing CISO more often, now.

Vijay: C-I-S-O stands for chief information security officer. So, it is really to help people like that build security solutions and architecture to deliver security solutions.

Suzanne: How do we help them to visualize these kinds of solutions? I have seen in your blog post that you use metaphors. You have got some conceptions. Why don't you tell us about some of the things you are using to help these executive-level officers understand what it is they are up against, and what kinds of solutions might be useful to them?

Vijay: The thing I proposed was really to come up with something called a cybersecurity portfolio, which helps describe all the cybersecurity capabilities they have. It is kind of a counter-framework to what Lockheed Martin released as the Cyber kill chain, to basically deliver capabilities to combat these threats.

There are different types of threats, different stages at which these threats come in. The nice thing that Lockheed did was to introduce cyber kill chain to show this actual chain of events that takes place for a particular compromise to happen.

The case I am making is, if you can break the chain, you actually broke the chain basically making it not feasible for them to complete. I am providing a number of different capabilities to help you break this chain.

Suzanne: What is it that made you choose domain name systems, DNS, as the actual target for building countermeasures to disrupt this cyber kill chain?

Vijay: The domain name system is kind of an esoteric protocol; a lot of people do not understand it. Just like in the blog post, I represent the radius of attack which you try an increase in combating and IED, the domain name systems is a very powerful one. This covers a huge number of portions of this kill chain that can actually disrupt communication, making, basically, malware ineffective. In either stealing data or denying service, whatever their objective is, it gives us a very powerful tool to cover a very large range of capabilities that they bring in throughout the kill chain. That is why I chose DNS, and DNS blocking works a lot like electronic jamming. It can actually kill DNS. It can actually make it impossible for communication to even initiate, which is a very good starting point.

I want to warn you, electronic jamming is something that people have taken too much to an extreme. Here, there are some limitations on what we do with DNS. It is not exactly like the physical world. It is more logical.

Suzanne: When I hear that we are going to have this large radius of effect, then I put my user hat on. I think about, *What are the effects on users when you are trying to use DNS denial as one of the ways of countermeasures in attacks? Are there implications for the user community that you are not going to be able to access valid sites that happen to have a DNS that is potentially malicious? We run into some of that, I think, in our everyday work right now.* How do you mitigate against that kind of effect?

Vijay: Definitely. These are some of the things that CISO-level people or vice-presidents of security struggle with because they see the user impact, and they feel paralyzed not to be able to do something. I walk through this in the blog post, picking some of the options that you have as to how we can steer the user community.

If you do not have a user community such as in a critical infrastructure location, then you have less of this problem. But if you do have both in the same network, you can actually choose how you would redirect the traffic and how you basically represent something to the user to be able to call the service desk and go through procedures to isolate and see if this is actually not malicious. How do we work on these limits [of error in this DNS blocking system]?

Suzanne: The idea of creating a white list, even though it has some properties that might make it seem like it is malicious, if it is on the white list, then it is something that I will be able to access and use in my work.

Vijay: Yes. The DNS blocking today has come a very long way. It is very mature. So, you can do white list before blacklist. There are concepts like greylist that you can do where you basically delay the response, which makes it very difficult for malware to respond, but a human being can respond to it. Much like CAPTCHA or reCAPTCHA, where a person actually makes a request so they can get through, but a malicious code does not know that this actually requires something to be done.

Suzanne: Right. There are some ways of making sure that the user community can still do their work. So, that is good. That is a big conflict a lot of times. We have very strong security needs, but users have needs for doing work. So, sometimes those are in conflict.

Since we are thinking about the CISO level, what are some of the other enterprise-level things that someone thinking about doing this kind of blocking needs to take into account if they wanted to use DNS blocking as one of their strategies?

Vijay: There are a number of different new techniques that people have done research on, that I tried to put in the blog post. One of them for example, is newly observed domains (NOD) [Newly observed domains is a way in the internet to find types of communications that has not

been seen before.]. The likelihood of newly observed domains, meaning a domain that has never been used by anybody to access, unlike google.com.

It is something everybody-accesses every day. It is likely that it is going to be malicious. We could actually put this in this greylist type-of scenario, and we get a very big effect of being able to say, *These domains are very likely to be bad; something like 99 percent of them are bad*.

There are service providers willing to sell you this type of newly registered domains, which makes it very effective for you to subscribe to a list and be able to find out if this is actually being used for a malicious purpose and block it.

There are a number of different things I highlight there. The trick is, like I show in the cybersecurity portfolio, from left to right, I try to go through different capabilities, DNS falls right in the middle. Within that, we have all these options about picking some very highly effective capabilities to block broadly what malicious code does.

Suzanne: Excellent. So, this is one of the strategies that really is implementable, not just a research idea. Do you have any examples of things that have been caught this way or that have been thwarted by using this strategy that you would be able to share?

Vijay: Yes, sure. Just recently, Verisign, Infoblox, and Farsight are three big providers who concentrate on this. They actually analyzed the WannaCry ransomware and found out different parts of the ransomware where they could actually kill it by DNS blocking. It is very simple to implement. The impact is very big because WannaCry is not able to encrypt the files before it starts its process of asking for ransom money.

Similarly, in the DDoS world, the Mirai botnet, for example, depends heavily on DNS to get its different parts of its malicious code back to a source. This is also, after the fact [After the initial infection that we try to contain the effect of this malware]. But if you had this capability in production in many industry critical sites, WannaCry, for example, would be very ineffective.

Suzanne: Well, anything that will make ransomware ineffective is a plus in most people's book. We talked about the enterprise level, but when we talk about ransom, more often that is targeted at individuals. Are there things that individuals can do? Are there utilities and things that they can use to enact a DNS denial on their own? Could I do that on my home network?

Vijay: Yes. There's many new providers, which have really sprung up. Some of them even provide free service for something like this. Open DNS is an example, which was recently bought by Cisco, and it is called Cisco Umbrella Service, now. It basically gives you a DNS white-listed number of domains that all people access. The likelihood of you having bad stuff

come back to you is very, very small, and you can use the blacklist to block even large categories.

Say you want to block pornography or you want to block file sharing protocols. You could pick those things as big buckets, big categories, under which at the very initiation of communication, it can kill those types of communication, either by policy or because of the risk these introduce to you personally or to the enterprise.

Suzanne: I think that makes us even more powerful because it is both an enterprise-level technology and a strategy and also, an individual strategy. We do not often see ones that go through that whole gamut. So, this is something that sounds very promising. Anybody that has been affected by some of these attacks, I think, will find it very useful to look at your blog post and take some action.

That is the thing, do not just read about it. These are all things that we need to all take action on if we are going to actually prevent these kinds of threats from occurring in the future.

What are some of the areas that you are working on now that are either taking this research further or new areas of research that we may see future writings from you on, Vijay?

Vijay: Just focusing on DNS, we actually have done the other side. We recommend—whenever we talk to the CISOs—much like Robert Frost's quote on putting up a fence, and then finding out why it was there. You do not know why it was there—we really recommend monitoring of this fence. To put a DNS firewall, it is like a fence in one way. How do you actually monitor it and how do you mature it?

The second thing, in the blog post, we are looking at it as basically analyzing what we call passive DNS. We can find out what is escaping this fence, possibly, and what are the techniques the adversaries are using now that they know you are using DNS blocking? What are they using to try to get around it?

Suzanne: This is a cycle.

Vijay: We did some analysis of DNS being used for covert channels, being able to ex-filtrate information out. So, that is something we are going to write on, soon. Then there is another side. If you do passive DNS and active blocking, now we have a full-loop control system.

If you look at it from that electrical engineering like side, you can actually measure what is escaping and keep feeding it to reduce the amount of risk that are continuously introducing regularly to an enterprise. So, those are the ideas we have for the next few blog posts.

Suzanne: Excellent. So, I look forward to those. I did not expect that this is something that would be applicable personally. Now I am going to have to go find out about the tools that I can use because I have not been a victim of ransomware, yet, and I do not want to be. So, I am all in for that.

I want to thank you for joining us today, Vijay. I want to point our viewers to your blog post, which can be found at insights.sei.cmu.edu. I think if you just search on Vijay, V-I-J-A-Y, you will not get too many other Vijays out there that are writing. You could also go to Sarvepalli, S-A-R-V-E-P-A-L-L-I. That probably will guarantee to get only this Vijay.

I do thank you for joining us. I do want to remind our viewers that you can find this podcast on the SEI website at sei.cmu.edu/podcasts and on our YouTube channel. We do have one. You can also find it on the Carnegie Mellon iTunes U site. As always, if you have any questions, please do not hesitate to ask at info@sei.cmu.edu. Thank you, for watching.