TRANSCRIPT FILE

JULY 19 Overview of Commerce Department Botnet Report and Roadmap

>> For those of you who are interested, we're going to use the next 20 minutes or so to talk a little bit but a government-wide effort that's been happening over the past year on distributed automated attacks, and for that, we have my boss, Evelyn Remaley, who's the Deputy Associate Administrator of NTIA, and Adam, who is the guy who seems to run this.

[LAUGHING.]

>> Good afternoon. It is very nice to see all of you. Thank you very much for coming to our first multi-stakeholder on this topic, and also thank you for allowing us to take up a little bit of your lunch here. We did just want to come and talk a bit about where we are after the release of the Botnet Report, which came out in May. The Botnet Report was a tasking that was assigned to the Department of Commerce, NIST, and NTIA taking part in that, as well as the Department of Homeland Security under executive order 13-800, and what that asked us to do was to work with stakeholders to look at developing a report that looked out at how to improve resiliency across the network and also to get at the issue of combating botnet's and other automated and distributed attacks.

And so, we spent a year. We came out to stakeholders last July with the request for comment asking for feedback on things in this area that had happened in the past, what was working well, what had changed in the landscape, and where we needed to go. And, obviously, one of the big drivers for why this was included in the executive order was the fact that there was an understanding on the government side that IOT, for an example, was really changing the landscape, and although we had done some good work on botnets in the past, that this was changing some dynamics in that it was time to relook at how we were actually working together as a community to combat these threats.

So, we spent a year developing the report and released it in May. So, I am going to, in just a few moments let Adam talk about how we're starting to move out on the report, but one of the key things that the report called for in May was the development of a roadmap. So, the report itself came out with five top-level goals that we identified through stakeholder feedback that we needed to concentrate on this area to make progress. And then, under those goals there were about two dozen action items.

When we came out with the draft report in January, we received very positive feedback, and a lot of community consensus that we had targeted the right action items, but there was a lot of concern about how we moved out on this in a very structured way. There was concerns about prioritization and really aligning resources and questions about what actions should come first, what actions built on others, and so there was a request

that as we moved into the next phase of that activity, that we prioritized and really moved to that implementation stage.

And so, that's what where here. That's what we're doing now. That's what we're here to talk about today. Immediately after the release of the report, the report called that we would develop a roadmap, so this more specific implementation approach in about four months, and so we just kicked off that activity last week, after having a lot of interaction with the White House in terms of their priorities and where this effort fit in. And so, that's where we are today. We're getting out, talking to stakeholders about what the botnet roadmap is. We're trying to get feedback in terms of what the levels of effort should be in that document, how we're going to work together as a community to implement these actions, who in the community is already taking action in this area, so that we can reflect that in the report, and also working internally, as a government, to identify the actions that we'll be taking and mapping out how we'll resource those and how they tie into other activities that are underway.

One of the key activities is actually the session that you're at today, so NTIA, this was one of the one areas that were called out in the Botnet Report that we would move out on the software component transparency multi-stakeholder process, so this is the first action item that we're kicking off that fits into the botnet roadmap.

So, with that have longwinded overview of the Botnet Report, let me also turn to Adam, who's going to talk a little bit about what NIST is doing and has underway on the IOT line of effort for the roadmap as well.

>> Sure. And thanks to Alan for giving us a few minutes to talk about this. So, you know, one of the comments that we got moving to the roadmap that caused us to put the roadmap in was the sense that a lot of these actions build off of one another, and I also think the thing I really like about the comments to the roadmap are the sense of accountability, so understanding the timeframes and the fact that this is an ongoing process and that we will come back at some point to assess what progress we've made and sort of how we have to modify implementation.

The other challenge that we always have in these spaces is that we're looking at ecosystem-wide problems, so how do we really scope everything that's in that ecosystem. So, even at NIST, we talk about our IOT program, and there's, in some ways, everything we do in cybersecurity should have an IOT component.

But we do have a specific security for our IOT program, where we are defining what those initiatives are that we consider in that bucket. We had a workshop last week on the 11th. I think many of you were probably there. I wasn't, so you can probably tell me what happened, better than I can tell you. But part of that was on some ongoing work that we have to develop a basic guide for departments and agencies, using leveraging our FISMA authority on IOT security and privacy risks, so we've shared several drafts, and we've had several working sessions, so that's an ongoing project, and some of the discussion last week was on that draft.

The report also recommended looking at security profiles for specific types of products. Another thing that we got as a comment and something that will like to hear is building off things that are already working, so part of our initial effort is to look at those existing security profiles that have been developed. The report actually lists a few, so that's something that we're assessing and considering.

And then, it's also looking at voluntary tools, so I think part of what we're doing with the roadmap is starting to identify, you know, what is the work that industry's doing? What is the work that certain groups would like to do, to the extent that we can document that and then have that be something that maybe in the future gets built off of, so, you know, people talk about the energy STAR concept for IOT. If those things are being developed, then it's helpful for us to know about them, and then in the future, if that's something that drives government procurement, then that's something that the report sort of highlights, but as we move into the implementation phase, we need to know what those sorts of things are, how they're progressing, and are there things that we can do on our end to help that move along?

So, that's where we are right now. I think more information to come, and happy to answer any questions.

>> Yeah. And just give a sense of next steps before we go to questions, so we are right now in a writing stage at NIST, NTIA, and DHJ to pull a draft roadmap together. Our hope is to get a draft out to the community sometime in September, and then, based on the timeline that was set out in the report, we're striving to complete, to have a final in mid-fall. So, we are, right now, in that very heavy data-gathering stage. That's why we wanted to come here to talk, but we are also having smaller meetings with community members to hear about other activities that are under way.

As Adam mentioned, really, one of the key goals that we have for this implementation stage is about accountability, but it's about each of us in the community being accountable to one another and being able to really talk about what work is already happening and to reflect that in the roadmap, and so the plan is, and was required in the report, is that once we publish the roadmap, we'll then have a year to work on that implementation, and then we'll come back and report back to the president in one year on the progress we've made. So, during that year, we'll get back together with the community one or two times to check on progress, to get an understanding of the barriers that the various work streams are facing and to make up dates to the roadmap during that time as needed.

What Megan has up here on the screen are four of the level of efforts, lines of effort, but thank you Megan, that we have identified so far, and you can see some of the action items that are falling under there. If you look at the report, if you need a copy of the report, please reach out Allen, Megan, Adam or myself. We can get that out to you, but you can see how we're starting to fill in the actions that will occur under these lines of effort. And with that, yes, any questions that you have for us?

>> I think there was one other thing we wanted to mention, which was if your organization is doing anything that aligns with these lines of effort, or if you look at the Botnet Report and you see an action that you guys are contributing to the solution there, please do let us know, because we'd like to make sure that that's looped in with others who are working on the same efforts.

>> Sure. Go ahead.

>> Does your IOT include mobile devices, or do you have best practices involved for mobile devices?

>> I believe so. Yeah. I mean we don't have a, we did not go the path of defining what IOT is, but I think our guidance is inclusive of that, and we have separate mobile guidance as well.

>> Yeah. The main reason to ask that was we at SEI, we've been researching over the year updates model for IOT. Certainly, we have interest to you, because it intersects between mobile and IOT.

>> So, that's absolutely the type of work that we would be interested in talking with you about, hearing about, to see if we can fit that into one of the broad action items to show progress being made in that area.

Yes.

>> Kent. So, the coalition's working on the DDOS profile that she had listed up there. One of the things that I think we made need at some point this summer, and I'm sort of asking the question to see if it's possible is try to figure out an avenue or an event where we can really expose what we've been doing. We feel it's reasonably mature. It still has some work to be done. We're adding some of the 1-1 kind of efforts that need to be incorporated into it, but having an event where we could bring that and have NIST then or NTIA make it public so that they could be in a bigger tent, so to speak, more people looking at it, more people reviewing It.

>> So, I will say that that is what we are envisioning for those. When I was talking about the meetings that we'll have throughout that year, is that we're envisioning those as an opportunity for the community members who are working on these action items to come and to talk about the progress they're making, what they've been doing, to bring some attention to that. So, as a community, we're getting an understanding of how the progress is moving forward, and then, to make the connections needed, so if there, you know, several different activities occurring under one line of effort to make the connections possible, so I don't know if that sounds like seeming that would --

>> I think it would be useful. I'm more, I'm not really too focused on the status aspects and letting people know what's going on. I'm focused on the content aspects and

wanting to have more expert reviewers outside of our circle, and we have some really great experts there, but you know, the bigger the tent, the more people can review it, the better the product's going to be.

>> Yeah.

>> Yeah. So, we'd be happy to strategize with you on that, what the right audience is, what the right venues are. I mean even, the reason why Evelyn and I are here is because we were initially talking about how do we bring in stakeholders to the roadmap. We considered doing a separate event, but then we said, "Wait a minute. We're going to have a good chunk of the audience at NIST on the 11th and another good chunk of the audience with some overlap here on the 19th." So, you know, we will look for those sorts of events that we can bring in if we think the audience is there minimize kind of burden, but to the extent that we think we can fill out an agenda or do an event to bring in and get that engagement, that's certainly a pretty good tool that we have.

>> Yeah.

>> Thanks.

>> In your lines of effort, I'm not sure what labeling refers to under internet of things.

>> Right.

>> But I'm going to make a guess.

>> That's good.

>> Conformity assessment Labeling.

>> OK. Then, that's not what I was thinking. What then to have you be aware of a couple efforts underway that we could use some level of standardization/community effort around is being with the just know what is that internet at the end that's communicating with my environment, and so there are vendors that are creating their own propriety databases. There are academics that are trying to do this as well. There's practitioners that are doing it too, but there's no, well, one place where we could collaborate and share, a single place where we can have a profile of a device that gives us a pretty good understanding of this is what is it. This is what version it is. This is what the function is, and then that will help us understand what we do about It.

>> So, NIST has been doing some great work around an IT drafted standard called MUD - manufacturer usage description, which is a standardized way of pointing to a traffic profile, but they've been, I think, great at saying this was not just about that one aspect, but looking at these superset of how we can use --. We can take advantage of the fact that devices are much simpler than general purpose computers, and we could empower the edge to do some of the security lifting for us.

>> We can get you that. We can get you that information and connect you with the folks working on that.

>> OK. I wasn't aware of that, and that's good, so that what you're telling me and what I should do is if I see anybody doing anything different, I go yell and them and tell them, "You should be using this, following this standard."

>> There is certainly value for fingerprinting, especially for legacy devices. The manufacturer usage description is going to require, you know, on device additions, and so, but teeth vision here, the challenge is how do you empower your local router to actually make decisions, and so there's a broader discussion. We certainly don't want to have, say that the fingerprinting stuff is useless, especially for things that are on the market Today.

>> Yeah. The approaches that we're seeing doesn't require any modification to the device. It's essentially saying based on who it talks to, the frequency, the protocols it uses. We believe that this device is this of this version

>> Yeah. And this is Eric Winger from Cisco over here. There was a kick-off meeting. Was it last week? At NTIA about this project, and there were discussions as well about how to deal with this brownfield space and whether or not you could generate something that's akin to a MUD - manufacturer usage description - but that would be generated by observing a device where you don't have that information, so in that kind of case, the information from the manufacturer would be the most authoritative source of information, but you might be able to still drive information in the same format with maybe a little less authoritativeness by observing how devices act, and so there were discussions about whether or not you could essentially generate those sorts of files.

>> Yeah. And essentially just to give you a sense of how we would do it, upon the intake of a device of some sort, we would profile it and say, "This is what we expect this new thermostat to do," and so if we start seeing that same traffic, we know it's our thermostat. But that's not an intake, because the manufacturer doesn't provide that to us.

>> Right.

>> If we had a centralized place where I could see some behavior and then quickly say, "Oh. That's a Chinese camera that's operating in my network somewhere," that's what I want to know.

>> Right. And so

[indiscernible]

>> Yeah. No. So, but I will say overall that that's one of the things that I really like about the approach that we ended up here is that we're not just looking at the devices themselves. We're looking at enterprise needs as well as the entire ecosystem, so, a lot of times you see their IOT strategies. They're all about the security of the device, which is an important piece, but we need to think about legacy and all these other components that we're really going to need to make progress.

>> Clete.

>> Hi. Clete Johnson from Wilkinson Barker Knauer. I just want to put in a plug for this process because watching it over the past year, it seems to me that it sort of is to the ecosystem and ecosystem challenges what the NIST framework process has been for enterprise risk management, and there's a big opportunity here to move the ball, move the needle significantly. So, I just wanted to commend you first, and second ask how do other parallel processes like this multi-stakeholder today, and also the NIST IOT workshop and the processes that are going on there along with other things like the DHS initiatives that are underway, the National Risk Management Institute and things like that, how do all these things fit together into kind of a coherent process?

>> Um hmm.

>> Or how can we, how can stakeholders help assist them to cohere into a coordinated Process?

>> Right. Do you want to go first?

>> Sure. So I mean at least two of the things that you mentioned will be captured in the roadmap. So, I think the whole idea of the roadmap is an effort to bring together these distinct effects and show how they relate or at least track them together to understand how making progress in one should have influence on another.

>> Right.

>> So that was kind of the idea behind the roadmap. You know, we'll never be perfect, and there will always be efforts that some people will think, "You guys are missing the boat because these things are more connected than you believe they are," but we're going to do our best, and we're going to figure out how to document whatever we think the consensus is and what makes sense to put in these buckets, so that's part of why we're here.

>> Yeah. And just, you know, taking that up to a higher level, I think we worked extremely hard on the Botnet Report to end with all of you, the stakeholders, to really map out what those coordinated actions needed to be, and, you know, this is, we're facing a complex problem that is not going to be solved by one quick action, and, you know, that's the, the report actually starts out with a series of findings which is, you know, in this space there's no one size fits all. We're not going to find a silver bullet.

This is a global problem. It's an ecosystem problem. Incentives aren't aligned right now. And so that's why what we're doing here is more formulaic. It's an approach. We can't do one action that we've identified and not do others and call it a success. But that's really hard for some people to understand. They want a quick solution. They would like us to say, "Top down certification is the way to fix this problem," but us working with all of you, we think this is the way we're going to keep the market motivated to and for all the players in this environment to be working together to find solutions, so, you know, I think Clete, you know, what we see is, you know, as Adam said, is that the roadmap is the way to show those connections between the activities, but we really do need to have a series of things that we're working on together and tracking to get to the endpoint that we need to be at.

>> Let us know how we can help.

>> Thank you. Thank you. Senichi.

>> Hi. Senichi from NTT. What is your current sense about the accountabilities among the communities and also stakeholders, and if you could have some strategy or ideas how to increase the accountabilities. Could you please share that?

>> Yep. So, I'll just start off with a few thoughts and hand it over to Adam. I would say that during this process, we have been, you know, really just pleased with how much community engagement there has been on this activity, you know, from the moment that we put out the request for common, the community has been engaged, and before, you know, we published the report at the midterm, and between the midterm and the final report, there were already ecosystem players, stakeholders out there starting, launching work in this area to contribute to the action items that have been identified.

So, what we're trained to do and, again, what we think is very important about the roadmap is to be able to show where that activity is happening and to be able to attract that and show that. Again, you know, the accountability to each of us. We've had government, civil society, industry involved in this effort, and we really all need to be accountable to one another, so the roadmap is a way to do that. But I do think it's worth saying too that we also started out this process with knowing that the stakes right now are very high. You know, we really need to, as a community, show that us, that the market is going to be able to work, that collectively, you know, the open standards process that we're all committed to is helping us to make progress, and I think that's why that we had so much commitment, and there's a commitment to go forward too is that everyone realizes that now is the time that we need to show, you know, we're seeing other regions of the world move in a different direction to show that this is the way that we can preserve the innovation but make progress on these hard security issues too. We need to do it together. We need to work together.

>> Yeah. So, I see accountability on the --. I agree with everything everyone said. The accountability is really on the government side, so specifically, you know, if you look at the report, I think the report documents pretty well that there have been previous efforts

in this space, and they produced good things, but by and large they didn't have the impact that they were intended to have. So, I think the report gives a really honest assessment of those previous efforts, so part of the accountability that was built in, and I would say the tasking from the executive order tracks pretty nicely with the recommendations from the Cybersecurity Commission, that they made a similar point, that there was good work done a few years ago with the industry botnet group and some other efforts. Really, we need to go back to that and build off of it. So, I think, when I'm talking about accountability, it's much more on the government side and to the overall effort. I have less concerns about accountability on the industry side because the way this was built, the reason why industry and outside stakeholders are doing it is because there's a value to them.

Often, the bigger challenge on that side is less around accountability. It's more around awareness and visibility. I mean I think even some of the discussions this morning or even just going back to Suno's question, it's like are people aware that some of these efforts are having, and even Kent's question as well. So, part of our efforts here are to provide accountability on the government end with our interagency partners, and then grow that stakeholder community, and make people aware of these existing projects that we think, that everyone thinks, could help with this overall Challenge.

>> Alan, did you want to call for folks on the phone. Is that --. Do we need to --.

>> Sure. Anyone who's listening on the phone bridge, and I see a number of you are that have some things to add or questions, you can hit *1, and then we'll be able to bring you into the conversation.

>> OK. Well then back to your --. Oh! Josh.

>> One more. Josh.

>> The Colombo question. Just one last thing.

[LAUGHING]

>> If this was covered while I was getting my sandwich, I apologize. Granted, you're legislative branch, excuse me, executive branch, there is that Senator Warner Gardner IOT bill, which in part was a response to [indiscernible]. I hear it's been massively reduced in scope, but how congruent are the recommendations from the botnet working group and your efforts versus the idea of no-fixed credentials or devices should be patchable or coordinated vulnerable disclosure is probably a good idea. Like those are the three concepts that seem to be stick through the fights. Are those people compatible with your work or -- ?

>> I think that the overall, I think, some of the recommendations in the guidance that NIST is covering does have some of those aspects in it, but it think it's just different in their mechanism because the Warner Gardner bill puts it through a procurement

process, and, you know, the NIST authorities are a little different under FISMA and developing standards and guidelines. So, I think there are similarities there. There are similarities in some of these other security profiles that we're evaluating. In some ways, it's just the mechanism that they have is different than what we do under FISMA with standards and guidelines.

>> But no massive points of diversions in Content?

>> I mean I think there probably are because --. I would have to go and look, but they're focused on three, and I think the guidance for developing is much broader, but I think there are some similarities that keep on coming up on recommended security protocols. It's kind of just the way that you enact and put it in the system.

>> Can you clarify the timelines? You did mention four months from when?

>> So, our timeline of 120 days kicked off last week at the NIST workshop was our kickoff for the roadmap timeframe, so we are shooting for September to get a draft of the roadmap out for comment and important from stakeholders, and then we expect to, you know, meet our deadline and wrap up in October.

Any other questions? Nope? Thank you. Thank you so much for having us, and please reach out to us as we said. Here's a central mailing list to give us feedback or to come in, or we can come to you to meet in person, and we look forward to further engagement on this. Thank you.

>> Thanks.

[APPLAUSE]