TechNJ Podcast Episode 2 (Bug Bounties) Transcript:

JS: Hello, and welcome to TechNJ. I'm your host, John Silvestri. Today, we're going to talk about hackers – the ubiquitous boogieman of the digital age effecting everything in our social lives. Politics, government, private business… stealing your emails, stealing your passwords, stealing your personal information, it seems like every other day we have an emergency involving hackers. And with systems becoming more and more complex and more and more interconnected, hacking is just going to become more and more of a problem – especially when the surface area of the attack grows and grows. So how do we combat this issue? Well, today we're going to be discussing bug bounties. I'd like to welcome back Krista Mazzeo, cyber threat intelligence analyst for the NJ CCIC, under the NJ Office of Homeland Security and Preparedness. She is a certified ethical hacker, and has a Masters of Science in Cybersecurity. Krista, thank you for joining us here today!
KM: Thank you for having me!
JS: Ethical hacker certification is the coolest certification I've ever heard of…
KM: That's why I have it!
JS: Tell me a little bit more about the ethical hacking certification.
KM: I had decided several years ago to kind of change career paths. I have a background in English and Communications, I have a background in commercial radio as well as college radio. Well I realized that wasn't going to pay too well moving forward, so I needed a better career path. I decided to pursue a Masters in Cybersecurity, because I knew at that point cybersecurity was going to be a very big thing very fast. Within the IT world, certifications are key. There aren't a whole lot of degree programs that employers focus on, and although I did want to get my masters, I wanted something else to kind of boost myself and improve my knowledge. So I had heard of the certified ethical hacking certification which was relatively new, and I took a chance and I thought, "That sounds like fun". So I signed up for a boot camp course out in Seattle, week long, took vacation from the job I was working at the time went out there, and just studied, studied, studied, studied, studied. Passed the course, got the certification, and before long I was starting to see it on job postings, as not so much a requirement but something preferred. The reason being is that certified ethical hackers have to work within specific parameters. It's beneficial for companies and organizations to find vulnerabilities in their networks and systems before the bad guys do, but it takes a lot of time, energy, resources and knowledge that your standard IT administrators don't have, and specifically with time. This is where you have ethical hacking, penetration testing, that's where that comes into play. And that way you can either bring in a consulting firm, and they'll test your systems and networks, see if there are open ports, see if there are vulnerabilities in your web applications, in your website… anything that hackers can use against you to get into your networks. So I decided that that sounded like an exciting career path.
JS: Also, you work for the NJCCIC, the Cybersecurity and Communications Integration Cell.
KM: Yup!
JS: Can you give me a little bit more information about what their mission is? What you guys do for New Jersey?

KM: What we are is the state's one-stop shop for all things cybersecurity. A couple years back, some people had this great idea of putting together teams of people with varying strengths in different areas and have them collaborate and work together to collect cyber threat information and share it among our partners, because the more information that's shared, the more we can help protect ourselves and others. So, we work alongside the Office of Information Technology, who works very hard to protect the Garden State Network and everything attached to it. We work with our partnerships branch, which includes a member from the New Jersey State Police. I formed a liaison with the New Jersey State Police Cyber Crimes Unit. We also have partners in Department of Homeland Security and the FBI. And I'm within the analysis branch, so we kind of take information from everywhere, open-source internally, and we form products and reports that we send out to our membership to alert them of indicators of compromise, and what the biggest threat coming up is, so that they can work to protect themselves.
JS: Sounds like a great idea for the state of New Jersey, make sure they have one-stop , as you said…
KM: We're really, you know, one of the few states that are actively doing this. And I believe we're the only state that is set up in the way that we are where we work alongside so many different types of people to bring all of that information together.
JS: It's always nice to have one place to go as opposed to, you know, having it in like little cells spread out as sometimes in a bureaucracy in the government it's hard to sometimes consolidate that knowledge.
KM: In government, one of the biggest problems is information sharing, and there's a number of reasons for that. Government employees tend to move around a lot, get promoted… so information sharing has always been a challenge, especially after September 11, that's when the government decided that hey, you know, our intel agencies really have to start working together. We can't be working in silos anymore, because that's not benefitting anybody.
JS: Bug bounties are a new thing that people and companies and organizations are using to kind of leverage the community. But what exactly is a bug bounty? What constitutes a bug bounty?
KM: Bug bounty, simply put, is a program that an organization will run, essentially a competition, opening up to a number of, you know, hackers, penetration testers, inviting them to find vulnerabilities in their websites, networks and systems. It's outsourcing penetration testing in a fun and unique way that, if well implemented, can draw some of the nation's top talent to you, especially if there are very good rewards involved. It's probably easier than contracting out to a small pen-testing company, and having a large number of people trying to hack into your systems, you're going to find more vulnerabilities quicker that way than if you're just working with a select few people.
JS: It kind of has a Wild West feel to it, sort of like the sheriff putting up the wanted poster. "Wanted: your bugs." You know, dollar signs available. See the sheriff.
KM: Cybersecurity is the Wild West, I'm telling you, right now. I mean, people are just hacking everything just for the sake of hacking.
JS: Government agencies has a public facing login, for example, they just say, "If you can find a bug in this, we will give you some compensation."

KM: Essentially yeah, that's really what it boils down to. This issue is, is that a lot of people, especially if organizations are running their own websites, they don't realize that, you know, you visit a website and you don't think anything of it. You think the files are stored on some remote server somewhere, someone else is hosting it… but if organizations are hosting their own websites, and have, say, a portal to log into, that invite members to create user accounts. Once you create that user account, that is essentially an entrance into your network. And if it's not properly segregated, and if it's not properly secured, you could have people rooting around where you don't want them.
JS: Sure, yeah you gotta make sure that your logins and everything, all your privileges and all your authentication and your authorization is all locked down and secure. What goes into the planning of a bug bounty? Like, is it just a simple as putting it out there and saying, "Hey, if you can break our website we'll give you $1,000?"
KM: Oh no, that is asking for trouble. That is asking for trouble. No typically, there needs to be a structure surrounding it. And there are a few companies out there that are providing that structure as a service. One company in particular that the United States Air Force is using and the Pentagon actually used last year called "hacker 1". Essentially, they contracted out to Hacker 1 and said "listen, this is what we want to do, we want to conduct a bug bounty but we need help in setting the parameters, setting the rules, facilitating the payments for vulnerabilities found, vetting the hackers that are going to be involved" - because that's also an important process. It's not… you're not opening up to the whole world and say, "hey, show us what you got", because you're going to have nation-state actors who are really going to take you up on the offer. And, you don't want that… but, you know, you need to set rules and guidelines, and that component is outsourced. And from my understanding, hacker 1 and these other bug bounty programs are very good at doing that.
JS: Is there potential for, say, somebody nefarious using a bug bounty as kind of a shield? Like, "oh, I was just pen-testing, I'm not really trying to steal you PII…"?
KM: Absolutely! In fact, there was a case – Facebook had launched a bug bounty, and there was an issue where a "security researcher", quote unquote, discovered vulnerabilities in an Instagram server, which exceeded the scope of the bounty. And he was ultimately threatened with legal action by Facebook. And Facebook even contacted the CEO of the company the guy worked for, and it nearly costed him his job. So there are risks to both the participants and the company hosting it or the organization hosting the bug bounty, especially if you are allowing hackers to, say, port scan and, you know, penetrate your network that way. A hacker could come along and hide in the network traffic, figuring that nobody's really playing close attention, there are a lot of IP addresses flying around, that he's not going to get caught, so yeah, I always encourage people to make sure they monitor their network traffic closely. You know, even look into white-listing IP addresses, something along those lines. There needs to be some control or else you're going to have a problem. There is a risk, but I would say overall the benefits outweigh the risk.
JS: Okay, so you could even use, as you just said, you could use a bug bounty as a potential smoke screen. So, there's so much activity going on because people are looking for bugs, the one person whose just looking to get in and be nefarious about it is gonna get lost in all that traffic potentially if you're not aware.

KM: Right, and another way to kind of prevent that or protect against that risk is when the bug bounty is implemented, make sure there's some kind of gag rule. Hacker 1, I think, will kind of scan twitter accounts. When you submit an application you going to have to reveal what social media accounts you have, because if you're participating and you say, "Oh, I just found this vulnerability in this website or this platform for this company, and it hasn't been patched yet, and you haven't actually revealed it properly to the organization hosting the competition, then that's going to be a problem. Because then that's out in the open, anyone can come along, grab that information, and use if for bad purposes. So, you need to kind of keep a gag order saying, "listen, you can't talk about these vulnerabilities you find until after they're disclosed to the organization, after the organization has patched them, and then let the organization reveal what those vulnerabilities were.
JS: You also mentioned there about having, basically, sign ups. So, instead of having just a wide-open bug bounty, having like a sign up and a list and a registration. That way, you know who's attempting to get in.
KM: You need to vet the applicants. You want to know who they are, where they're coming from, and I know typically the image people have in their heads of a hacker is, you know, somebody with their face covered, wearing a hoodie and gloves typing on a laptop because that's every stock image ever used for hackers.
JS: Well because all laptops come with that little camera now, so they can see you through the camera. You have to wear the balaclava or whatever…
KM: You just put tape over the camera, you know, that's what we all do now. But no, that's the thing, where it's, "ohhh, anonymous". Well, you don't want those hackers to be anonymous. And in certified ethical hacking, you certainly can't be anonymous.
JS: Sure.
KM: There's no point to it, and really, you know, you're kind of looked at it, you know, with a skeptical eye, like "why, what are you trying to hide"? If you're open about it, there's no problem. But yeah, proper vetting… I don't know the full ins and outs of their vetting process, but they could very well conduct background checks or, you know, use different databases to see does this person have a criminal history, have they ever been, you know, arrested or convicted for a crime involving computers or technology, and eliminate them from the competition.
JS: Typically, when we hear about a bug bounty, we hear about compensation, it's usually monetary. It's usually, "oh, we'll give you a range of x to y dollars, depending on the severity of the bug that you find". Is there other methods of compensation? Are people looking to put this on their resumes, for prestige, public acclaim?
KM: Money is the greatest motivator, and most of the bug bounties I've seen offer monetary rewards. And the reason being is that anything less than that, you're not going to recruit top talent. Especially in today's gig economy. That could very well be part of somebody's income that they do for a job in addition to other side projects. You know, scholarships could be offered but you're going to get a younger crowd, you're going to get a less experienced crowd, and most large organizations, they don't have time for that, and they don't want that. You want to recruit top talent, and money's really the driving factor for that.

JS: So are bug bounties a good stepping stone into the larger security world for computing? Can you use this as like your intro?
KM: It certainly can be a great stepping stone and a great resume builder. I'd certainly put it on my resume if I participated. Especially some of the larger ones… I mean, hack the Pentagon? Yeah, you want to put that on your resume. Hack the Air Force? Yeah, you want to put that on your resume.
JS: (laughs) As long as it's a bug bounty…
KM: Right, exactly, exactly… depends on what job you're going for. But, absolutely, and I think people do use that. Hackers in particular, and a lot of cyber security specialists, they like working for themselves. They like working from home. So, as far as them going after your nine to five desk job, they may or may not want to go for that. But still, it's good to have on your resume, especially if you are operating your own business. You can, you know, say to a client, "hey, you know, I found these vulnerabilities for this organization. I can do the same for you".
JS: We've talked a lot about what a bug bounty is. How it's implemented and everything. Has it been successful? Have we had good bug bounties, you know, fulfilled? Discovered?
KM: So last April, like I mentioned, the Pentagon did launch their own "Hack the Pentagon" bug bounty. It was the first U.S. Government-sponsored bug bounty of its kind. It ran from April 18 to May 12, and they partnered with Hacker 1. Some interesting stats here: it took just thirteen minutes from the start of the competition for a hacker to submit the first vulnerability report, and ultimately they received two hundred reports in the first six hours. Over fourteen hundred hackers registered and applied for the program, and seventy five thousand dollars-worth of cash rewards were paid out to the participants. One hundred and thirty eight of the submitted vulnerabilities were found to be legitimate, unique and eligible for a payout, and hacker one facilitated the payments to the participants. They ultimately found it to be so successful they expanded it to US Army websites as well
JS: You say, you know, they found a hundred and thirty eight qualifying bugs in the bug bounty contest for the Pentagon. But what happens if I am a hacker and I submit a bug bounty to Facebook, or to government, or to whomever and they're like, "that doesn't really qualify as a bug". Has there ever been a situation where there's been a dispute about a bug bounty?
KM: I mean, I don't have specific examples, but it's certainly a first-come, first-serve environment. So the first person to submit a unique, what they consider to be legitimate, vulnerability report, gets the payout. And then even if you find something that someone else found later, you don't get paid. But those rules are clearly outlined.
JS: For the hackers involved, you have to be at the top of your game.
KM: Exactly.
JS: So what are the kinds of bugs found during a bug bounty contest?
KM: Some good examples that are typically found include a cross-site scripting vulnerabilities. They're typically found in web sites and web applications, and it's essentially a way for hackers to inject malicious code into a website, so when a legitimate user visits it, their system become infected. For instance, if your web site publishes articles and allows reader comments or contributions, you have to make sure they're not able to load malicious scripts into the comment section. You also have cryptographic design flaws that allow hackers to steal cryptographic keys and forge authentication tokens in order to gain unauthorized access to your data. Open

ports are a big one. They could allow hackers to gain access into servers and networks. And we're seeing a lot of that right now with ransomware attacks in the state New Jersey. Organizations have no idea that the remote access ports are open and exposed to the internet, and tend to only find out after a hacker has brute forced their way in and deployed ransomware across their entire network, crippling them for days or even weeks. So there's also unpatched or vulnerable web platforms that are used. Certain popular web design platforms tend to be very vulnerable and seem to be pushing patches and web updates regularly. If the web site administrator hasn't applied those patches, then the website is open to defacement more. There's also problems with user authentication that are found, it's often seen in web sites that allow users to create an account. Passwords might be sent in plain text and not encrypted, so someone snooping on the network could easily steal them. And web user sessions might not time out, and be vulnerable to takeover by an unauthorized user.
JS: Definitely a lot to consider, considering that stuff is not getting any simpler as we get further and further here with technology.
KM: Just more and more interconnected, more and more complicated. Think about how many devices you have that connect to the internet now. And especially with smart home devices, you have security cameras, you know, toasters, refrigerators…
JS: Thermostat.
KM: Yeah, thermostat…
JS: It's the internet of things, everything is growing and it's just a bigger, bigger surface areas every passing day.
KM: Exactly.
JS: Well Krista, thank you for joining us here today. I appreciate your insights, I appreciate your knowledge. Thank you for coming in…
KM: Thank you.
JS:… and talking with us here on TechNJ. That'll do it for today's episode. Did you like what you here? You have questions or comments you'd like to send us? Send us an email at Podcast@tech.nj.gov. For TechNJ, I'm John Silvestri. Thanks for joining us today.