Darkweb

Guest: Krista Mazzeo

JS: I'd like to welcome back Krista Mazzeo to the podcast. Krista, thank you for coming on to the TechNJ podcast.

KM: Thank you for having me, yet again.

JS: Absolutely, it's always a pleasure. So something's been bugging me since the last time we talked…

KM: Uh oh

JS: So, there's all these nefarious people out there, we talked about ransomware last time specifically, but I mean, I guess it could apply to the broad security realm. There's all these people doing all these nefarious acts out there. Why isn't it just, obviously they're connected to the internet, they have an IP address…what makes it so hard to track these people down, and just apprehend them in the act of ransomware and such?

KM: Well, because they're using anonymizing technology that hides their location. They're not coming from an IP address that is attached to their home or place of business. A lot of people operate overseas in countries that are not friendly with our law enforcement efforts and these countries don't care if their people are hacking others outside of their countries' borders, so they kind of look the other way as long as they're not hacking their own governments, their own citizens. So there are a lot of technological challenges that come along with tracking down criminal activity online. And, especially with the use of the Dark Net where their added encryption and anonymizing features - that people are smart enough to use - to hide their tracks.

JS: OK, you covered a lot there in a short time. The first thing that caught my attention…the Dark Net. What is the Dark Net, how do I get to…not me personally, I have no desire to go to the Dark Net…if I'm nefarious, how does one access this Dark Net, can I Google search it?

KM: Well, there are a number of Dark Nets, we'll talk a bit about Dark Web…there are minor differences. There's also Deep Web, you'll hear that term thrown around a lot. And there's a difference between them. I'll start of by explaining that, because a lot of people get confused. The Deep Web is essentially anything that is not indexed by search engines. Meaning, search engines such as Google or Bing or Yahoo. They have crawlers - web crawlers that go out, and search surface pages for keywords. You know, Search Engine Optimization, you might hear that term. Businesses use them in order to be located and discovered easily online when you do a search for a term. Deep Web is anything that kind of exists beyond that ability to discover. For instance, when you log into your bank account online. I can't run a search for your name and your bank account number and have it come up because it's hidden behind a login screen. There are a number of things that are hidden behind pay walls or such that you need to login. Those pages are not indexed by google, by search engines. The Dark Web is kind of a portion of the Deep Web, it's kind of the underbelly of the internet, so to speak. Dark Web, you need - and Dark Nets in general, there are a number of different ones – you need special software or technology in order to access them. Whereas Deep Web, you can use your regular web browser. If you're using Chrome or Internet Explorer or Firefox, you can use any of those browsers just to go on your bank's website and log in.

JS: So, the Deep Web itself is not inherently evil, let's say – or bad. It's simply stuff that you can't access from a Bing search, a Google search, a Yahoo search...

KM: Exactly. Most of the internet is Deep Web.

JS: OK, so it's sort of like the iceberg. 10 percent you see on top, 90 percent's underground…

KM: …exactly…

JS: …or under the ocean.

KM: And the Dark Web is actually a subset.

JS: OK, so the Dark Web is a subset…

KM: …it's like the bottom of the iceberg, but nobody sees…

JS: …OK, that's the Marianas Trench…it's way down there…

KM: Exactly.

JS: So, you said you need special technology – you can't - I can't go to my internet and type in an IP address…or type in some security through obscurity, like I can't just go there knowing the password…it requires additional technology, you said.

KM: Yes. For instance, the Dark Web that most people talk about is – if you've ever heard of TOR. T-O-R, it stands for The Onion Router. And essentially, that the most popular of the Dark Nets. It's very easy to access. There are a couple of additional challenges, but it's still easy. And it's free. You just have to go to the TOR website and you download the TOR browser. It's a special browser. I believe it's based on Mozilla's Firefox because that's all open source. So it's a modified version of that browser that recognizes the domain names that are used on the Dark Web because you don't have dot coms, dot e-d-u's, dot govs, dot nets on the Dark Web. You have domain names that end in dot onion.

JS: OK

KM: And it's named that way because TOR is The Onion Router and they look at it as; you're peeling back layers of an onion to, you know, get to the source. It's kind of their cutesy way of describing encryption.

JS: OK, so how exactly does The Onion Router work? I mean, it just sounds like I'm downloading an application on my computer but in and of itself, that doesn't sound super secure.

KM: It can be dangerous. It can, depending on where you're downloading that browser from. You could get a compromised copy that reveals who you are. People have been talking about that. But, fundamentally, when you download the browser – what it does – you have two options. You can use it as a client or you can actually run what's known as a TOR node. And if you're running a TOR node, you're participating in the existence of that Dark Web. Essentially, you're agreeing to allow network traffic to run through your internet connection, your router – from other places in order to get to its final destination. And why that is, is because when you log onto TOR and you visit a Darkweb website, you're not just going from point A to point B. You're not visiting that site directly. You're going through a series of ten hops – as we call it – through other people's connections to get there. And every thirty seconds or so, that network pattern changes. So you're not logged in through the exact same connection for the entire session that you're on. You're actually switching nodes that your traffic is going through, which makes it very, very hard for law enforcement to trace back the source. Or trace users without extensive monitoring or without, you know, injecting malicious code into a TOR browser ripoff, so to speak, and revealing the end user that way.

JS: So, there's this Dark Web. Obviously TOR and other applications are enabling people to converse in a way that law enforcement can't easily identify.

KM: All right, and I forgot to bring up the main point is that these connections are encrypted.

JS: So, in addition to being randomized, network-wise, each hop is encrypted?

KM: Yes.

JS: OK, that's just…

KM: …and on top of that – if you really want to go deep – most people use what's known as a V-P-N or Virtual Private Network to connect to TOR. And the reason why is because your connection to the initial TOR hop is unencrypted…

JS: …Ah…

KM: …the way to encrypt that connection from your machine to that first hop is to use a VPN. So that kind of, diffuses the trail a little bit more.

JS: So, we have people using the Dark Net, various Dark Nets in this fashion…what's actually going on in these Dark Nets? Why does law enforcement care that people are talking anonymously?

KM: A lot of illicit activity, unfortunately. Now, TOR was actually created by the US government, the Navy. So, it was created to establish communication with you know, dissidents, political dissidents from other countries. It provides a way for people living in oppressive countries, under oppressive regimes, to communicate, you know, to law enforcement, to other sources. So it was created for good but like any tool, it can be used for evil. There are a lot of – I spend, I wouldn't say a lot of time - but for work-related purposes, I do go on the Dark Web just to see what websites are popping up, where people are going, what's popular. And there are a lot of forums. There are people that discuss privacy rights and they're privacy enthusiasts. And they might use TOR just to visit everyday websites. it's just, out of principle. Especially with all the digital tracking that goes on day-to-day from businesses and companies. I think a lot of people were getting fed up with that. So they use TOR as a way to deflect that type of tracking. However, a lot of people who are into – especially drugs – selling, buying, using. They've found that the Dark Web is a way that they can obtain a wide variety of drugs, very easily, and safely because they're not relying on their neighborhood dealer to get the drugs. There's no face-to-face interaction. Everything's done anonymously online. They figure out where to ship the drugs. They ship them there, and done deal. And I think that was driving the appeal and the popularity over the last several years with the use of the Dark Web.

JS: There's still the human element, right? I mean, people are going onto the Dark Web, but unless you know how to access whatever their domain name is…dot Onion. I mean, there still has to be some human element, some transaction…how do I get here…do I have to know a guy or something like that, you know…

KM: …exactly. And that's a good point, and people love to talk. And people love to talk online. And there are plenty of what we call Clear Web. That's the regular, you know, normal people internet, Clear Web. Sources that list domain names of, you know, active drug markets and where you can get this and where you can get that. There are also a lot of online forums and discussions about that. And people are very open about it because there are ways to be anonymous on the Clear Web, too. So if the website that you're using, the forum that you're using, does not keep logs of their users and people who post on there, then you can kind of get away with talking about whatever and it doesn't get traced back to you, if you're smart. So, they do talk about it: the Dark Web is not indexed like the Clear Web is. There are a few search engines that have developed recently – they're not great – it's difficult to track Dark Web websites because of the fact that they could be up one day and gone the next. It's constantly changing, it's not like on the Clear Web, when you have an online store you go to all the time and you know it's going to be there tomorrow. And you know it's going to be there next week. Dark Web is not like that. If a Dark Web illicit goods vendor is starting to feel the heat, they might take their website down. They also, might be taken over by law enforcement – which is timely that we're talking about this – because there was the very large AlphaBay Dark Web market takedown by international law enforcement efforts just yesterday.

JS: So, with all this anonymity - I was going to follow up with this – how does law enforcement get that foothold? How do they get in and bring it down from the inside, you know, the undercover sting, or something along those lines?

KM: It's tough. And, you know, I wish I could say they have this magic wand – magic technological wand - that they can wave and reveal the identities. However, usually – nine times out of ten – it's because the user made a mistake. And they weren't practicing proper OPSEC. In the case of the AlphaBay Dark Web takedown, it was revealed that, I guess, in the initial stages of him setting up this AlphaBay market, he used a Hotmail address. And Hotmail maintains its logs. He did not use a VPN or any kind of anonymizing technology to log into his Hotmail account. However, he had it connected to the AlphaBay market and he had it connected to his LinkedIn profile. So…

JS: …I mean, you got to get your resume out there…everybody's trying to build a good resume…

KM: It was tied to a company that he created. So, it was stupidity on his part. If he hadn't made that mistake, I don't know if the bust would have happened. There are other ways, too, that law enforcement works together to, you know, track down some people that are buying and selling. There's one story that I know of where the post office - where a vendor was going to mail the package of drugs that he sold - happened to notice that this guy would show up every week wearing latex gloves…to drop off the package. And that's normally something you don't see. So, they contacted law enforcement, set up surveillance and they were able to figure out it was a Dark Web transaction. So there are little tipoffs.

JS: A combination of just good police work and good cyber security…

KM: …yeah…

JS: …coming together..

KM: Yeah, and once, especially if they catch a vendor and then they take over his vendor account on whatever website he is. Sometimes, that's part of a plea bargain. Sometimes, well, they're probably not given a choice…then all of a sudden, law enforcement has control over an already-established vendor account that's got high feedback ratings. Nobody suspects anything. They think it's a legit vendor and law enforcement can track deals made that way. So there's multi-pronged aspects of tracking these people down.

JS: It almost sounds like the table's turned. The hackers become the hacked.

KM: Yes.

JS: And now the security, and the weakest link is now on the bad guy's side and the good guys are the ones getting in and exploiting those weaknesses.

KM: Yup, they get very angry about that, too. Hackers don't like to be hacked…

JS: (laughing)

KM: …and even TOR. Probably about a year, year and a half ago, it was made know that there was a vulnerability within the TOR browser that could be exploited. And as soon as the creators and maintainers of TOR found out, they patched it. But nobody knows how long that went and who was using that vulnerability or who was exploiting it to find out who's using it.

JS: So, everybody: patch your software whenever possible, whenever those come out…

KM: …unless you're a criminal, don't…

JS: …don't forget.

KM: Not for you, no patches for you.

(laughter)

JS: We've been talking more about the real world implications of the Darkweb, you know, illicit materials and things being passed along routes anonymously because the communication's been anonymous. Is there a pure security risk from the computer side? Do people use the Darkweb for ransomware, do they use it for viruses, do they use it for D-D-O-S, things like that?

KM: Well, part of the issue with the Dark Web markets, like AlphaBay, that was the largest market – in fact, I think I have some numbers here – according to one AlphaBay staff member, they claim that the website serviced over 200 thousand users and 40 thousand vendors. Around the time of takedown, there were over 250 thousand listings for illegal drugs and toxic chemicals; over 100 thousand listings for stolen and fraudulent identification documents; and access devices, counterfeit goods, malware and other computer hacking tools, firearms and fraudulent services. And the issue is: If was just drugs or just you know, light recreational drugs…sure they're illegal but the real problems is, is that you know, potential terrorists go on these websites. They'll try and purchase weapons, firearms, explosives. You have a lot of child pornography so there's that aspect to it. Some markets allow it, some markets don't. You know, not to mention all the hacking tools that are coming out of especially other countries – won't name names but you know who they are. You know, plus the drugs like Fentanyl. I mean, New Jersey's especially seen a real problem with Fentanyl and overdose deaths related to Fentanyl. And a lot of this Fentanyl is coming out of China and it was sold with the intent to kill the end user. You know, kill the purchaser. So there's that aspect too, I mean, loss of life…potential, absolutely. And this is why law enforcement had to take action on it.

JS: So this is truly an across the board threat?

KM: Absolutely.

JS: Is there any advice you can give anybody, I mean, it's kind of hard to say because this is at echelons above. This is at law enforcement, this is international. Is there anything the average person can do or is there anything they should be aware of about the Dark Net? Like for example…

KM: …stay off of it…

JS: You know, if your kids are installing TOR…

KM: Exactly. Because you're seeing the demographics of crime change because of this technology. You know, the older drug dealers aren't going to be, necessarily, adapting to newer technology and crypto currency and the like. Whereas, the younger ones are. And parents might not realize that their kid is going on the Dark Web or they have TOR installed on their computer or even mobile device and who their kid's talking to because they're not going to be able to see a record of that on their computer. So yeah, definitely, parents should be aware of the Dark Web, talk to their kids. I mean, if they're able to get drugs shipped to their home or a neighbor's house or something along those lines – parents can be completely oblivious because they're thinking "My kid's home all the time, he's not doing anything. You know, he's in the basement, he's playing video games". Make sure you know what your kid's doing. Check their computers from time to time. Demand to see what software that they have installed. So definitely. Definitely, that's the big one right there.

JS: We're talked about all the negative uses for the Dark Web, Dark Nets and obviously, they're serious and they're here and they're persistent. But you did touch on something earlier and I wanted to go back to that. People are using this as a way of protecting privacy from people going, you know, you go to a website and they're tracking you. They're sending you ads. You can get more browser information than most people realize just from your normal Firefox or Chrome or Internet Explorer. Is there a place in the world for that kind of utility? Even, obviously the drawbacks are severe, but is there a place for a privacy advocate to say "Hey, I'm downloading this not to get drugs or anything, but because I just want to be private on the internet."

KM: Sure, sure and it's, like I said, it's not necessarily a bad thing. There's nothing evil about that. This is the hard part about being in cyber security right now because on the one hand, you're telling businesses and organizations and individuals to, you know, make sure they encrypt their files on their hard drive to protect from data exfiltration. You're telling them to practice good security, not post things publicly online, not to install every piece of free software and game that they come across because it's filled with malware. You want to look out for and protect people, but on the other hand, you know that the more people use encryption it's going to be harder for law enforcement to catch the bad guys. So there has to be a fine line in between and the encryption battles going to go on for quite some time. Not just in this country, in countries across the globe because the government wants back doors into everything. Well, as we've seen with the recent leaks, CIA hacking tools and NSA hacking tools that when you have the ability to back door into somebody’s server or system – so does everyone else. It’s just a matter of finding that back door. So, there’s still a big fight going on of who’s really responsible, you know, and should they have disclosed the exploits and vulnerabilities to the software developers. You know, but they can be used to catch dangerous people. So, that fight is, I don’t see an end to that fight actually. Again, when it comes down to it, privacy is important. You don’t want your identity stolen. You don’t want malware on your system. Stealing banking login credentials is big business for a lot of criminals. You know, there’s a whole economy based on it. So, you know, you just have to, kind of weigh the risks and rewards.

JS: The bell has been rung, and Pandora’s box has been open, and it’s never going back inside.

KM: Bingo.

JS: We’re living in the new world of the Dark Webs and the Deep Webs. Well, Krista, thank you for coming and sharing all that information with us, it’s been enlightening. And I appreciate you spending time with us here today on TechNJ.

KM: Oh, no problem. Thank you for having me again.

JS: Excellent, thank you.