Tom Byrnes of ThreatSTOP

Speaker1: [00:00:04.77] This is the Investor Connect podcast program. I'm Hall Martin and the host of the show in which we interview Angel Investors, venture capital, family offices, private equity, many other investors for early stage and growth companies. I hope you enjoy this episode. Hello, this is Hall Martin with Investor Connect they were here with Tom Byrnes, founder and CEO of Threat Stop using real time security threat. Intelligence to block threats at firewalls, routers and DNS servers isn't new, but until now it's required large security teams, expensive threat intel feeds and significant manual effort threats to our cloud platform using security automation to make it possible for companies of any size to defend their networks with real time threat intelligence. Tom, thank you for joining us. Thanks for having me. So what was your background before founding thread? Stop. What did you do before this?

Speaker2: [00:00:53.34] So my real background in information technology and security goes back to being in the United States Army. I was originally enlisted soldier fixing radios and then got involved and became one of the first people involved in deploying automation. When the army started doing tactical automation in the field, we had these networks that we were deploying. They were out in the middle of nowhere or in places like Bosnia and Herzegovina. And needless to say, they were under attack or they could be attacked if they were connected to any kind of public network. And some of the more famous things in the early 90s did happen where, for example, German hackers published some of our drone feeds on the U.S. Army. So we got involved in security. That really wasn't an awful lot of actual security tools available at the time, were to make something of ourselves in the process. I wound up becoming friends with and getting involved in a number of the people who later left to start different security initiatives, most notably Mark Sock's, who was the first presidential advisor for cybersecurity in the White House under Dick Clarke. So I got into the field by virtue of just being in the military as a civilian, I had been involved in networking as the CTO, organized ultimately, and then helped a venture capital firm called Enterprise Partners with a couple of companies because it was one of their earlier companies that was successful.

Speaker2: [00:02:19.80] Could I Pivot, which got bought by Intel. We invited SSL acceleration. And so having been successful there, I went off to help them with building new other companies and had a particular focus in information security because of my background. So I helped build a number of companies that you may have heard of, Breach Security, which is a company that I trust with a company called Net Swift, which got paid by Cisco and a company originally called Loch Ness Monster, which is now McAfee's version of quality. After the Net Swift Acquisition, I was helping out a charity called Grant Smart, which was the database of all the charitable returns for private foundations for the United States. For the IRS, the idea was we would take all these tax returns and indexed them to allow people who are looking for grants to find people who would give them grants, and they would then download the information and actually get a copy of a redacted version of the tax return so they know how to get hold of the people. Now, the thing about these tax returns is they tended to have the Social Security number of the high net worth individuals who endowed the foundation and their signature because most of these were smaller entities than the very large foundations you're used to. So hackers were constantly attacking us.

Speaker2: [00:03:38.04] I was managing this for a charity. We had firewalls and things that were donated and I was updating it with data from the Shield block list, which is a Sands initiative that was first one of the first real threat intelligence platforms out there. And some also some stuff from the National Science Foundation and the Army Reconnaissance Office that was being put out by Samarrai. This is a fairly long and involved and annoying process. There were some tools there to automate it, but they didn't work very well. And I hit on the idea of using DNS to pipe the information to an ACL so we could block stuff and it worked. And so that's sort of what became the basis of what now is threat stop was the idea of this open source tool for taking arbitrary threat intelligence and putting into a firewall so you could use it. I got back two hours a day of my life and so put it out on the digital mailing list and said, hey, I've done this thing. You're interested in using it. And next thing, I had three hundred people using it. So I realized I might actually have a company potential. And so that's how threat stuff came into being. It took quite a bit of time to turn into a real product, but and some grants for homeland security. But we got it done.

Speaker1: [00:04:46.17] Sounds great. So what excites you right now?

Speaker2: [00:04:48.87] I think that we're actually finally at the point where people realize that cybersecurity is not a nice to have, but a need to have. You know, security has been, as everybody knows, an afterthought in the design of the Internet, but it's really an afterthought in the design of just about every single system out there. And the people who have a lot of money can fix that with a lot of cycles. But the vast majority of people can't. And as we've discovered in the solar winds attack and other types of supply chain attacks, you're only as strong as your weakest link or the weakest link. The vast majority of companies is their suppliers and their customers, and a great many of those are small and medium businesses. What excites me is what Truckstop is about, which is making them have already an easy way to do the kind of things that well resourced enterprises do to protect themselves and therefore protect our entire economy from the criminals and nation state actors that want to steal everything we've built.

Speaker1: [00:05:48.08] That's a good point. It's no longer just nice to have as a must have. So you do a lot with startups and investors out there for the cybersecurity space. What's your advice for people investing in startups?

Speaker2: [00:05:59.01] I have a very, very finely tuned best filter. There is like any situation where there's a gold rush going on and there is a gold rush going on in cybersecurity. There is an awful lot of snake oil out there. There are a lot of people with very slick pitch decks and pitches that can be very attractive that really there is no there there. The most infamous one of those was Norse Corp, which was built based on entirely false technology, yet was that they were able to attract a very large amount of investors. They had people with a huge booth at RSA and the infamous Viking hats, and then they imploded and it turned out that there was really nothing there. And some of the founders of that have gone off and started yet another company, which they're now talking about. So there's a lot of a lot of snake oil out there. And unfortunately, the vast majority of investors can't separate fact from fiction. So I think they need to find themselves someone that they really do know and trust who can to kick the tires and see if it really works.

Speaker1: [00:07:01.11] But then on the other side of that table, what's your advice for people running startups? What do you tell them to do before they go out to raise funding?

Speaker2: [00:07:07.02] I think a big part of it is find product market fit. Don't try to scale too fast. You want to make sure you've got a cool technology. In many cases, you've done it because you wanted to solve a problem that you had. But don't go raise a ton of money before you turn around and show that there's really dogs who will eat the dog food and pay more than it's going to cost you to deliver the dog food. Don't don't quite pay more for delivering the product with pay more than it costs you to market the product because your costs are going to be much higher on the marketing side than the operating product side fairly quickly. But make sure that you can at least deliver the actual product, the minimal viable product in such a way that people will buy it and will use it and they'll give you the feedback on what's missing on it in a way that has a chance of profit. Because when you layer on the sales and marketing costs, on top of that, you better have a profitable product at the at the end of the day.

Speaker1: [00:08:07.45] Great. So let's talk about the cyber industry. How do you see the industry evolving from here?

Speaker2: [00:08:12.78] I think the industry is in the same place as the Internet industry was in, say, 1996. There's a lot of confusion around it. There's some very large incumbent prior large companies that kind of you would think are really part of what is is happening in it. So you had the large telcos and they were trying to get into doing Internet services. And it turned out that the only way they really were able to do it was to actually buy the startups that were doing it in order to get to to products that people would buy. I think that we've had different iterations of information security, but the network based security that we have now and the endpoint based security is all being transformed by two things. It's being transformed by, first off, cloud adoption and hybrid cloud adoption. And secondly, it's being transformed by Iot and bewailed. So no longer do you have the silos that people were able to access inside and covid and work from home has really, really accelerated that, that people are no longer inside of a fully individually protected and managed situation like in the company would normally have. So I think that there's a lot of opportunity in that space.

Speaker1: [00:09:22.73] What do you think is the biggest change you'll see and say, the next five years in the cyber space?

Speaker2: [00:09:27.72] Well, you know, it's kind of funny. Bill Gates infamously once said we usually overestimate what will happen in the two to five years and grossly underestimate what will happen in 10 to 20. I think, however, we've seen that we had the catalyst of covid and work from home, and I think that that is not going to get undone. So I think that the need to be able to secure any asset that you have, wherever it may be, and any user, whatever they're doing is going to be of immediate concern. And you're going to have to do what people have or what they bring and not by saying, OK, well, now you have to get all of this new equipment and all of this new software. And by the way, it has to be installed. So I think you're going to see a lot of changes in how technology is delivered. I think the days of installing software. And buying more hardware are pretty much done

Speaker1: [00:10:25.95] Well, great, well, there are a lot of challenges for the startup and the investor in the cybersecurity space. What do you see as the main challenge started SpaceX in launching their business in the cyber space,

Speaker2: [00:10:36.33] Rising above the noise floor. It's a big problem. There's a lot of, well, resources resource people who have a very vested interest in their existing cash cow businesses and they are not going to let go of them easily.

Speaker1: [00:10:51.00] And then for the investor, you talked about the challenge of evaluating the technology, but can you dive into that a little bit further?

Speaker2: [00:10:57.33] Yeah, I mean, the biggest one is, is does it work? Does it really do what it says it does? An investor should be able to to use it in most cases. I mean, these are businesses. These are people. They have the exact everybody has the exact same problem. It's just a matter of scale. Can you actually use the thing or do you know someone who can and does someone you trust?

Speaker1: [00:11:17.52] Try it so the metrics are there, penetration tests or other trials that investors can put these things through and get real numbers to see how well it did? Or is it just not hard to not easy to rebuild a whole network for testing like that?

Speaker2: [00:11:32.31] Well, in most cases, as I said this, if you look at the really big theme, it's it's going to be not so much build a whole network to test it. The days of it being inside of a controlled environment are kind of done. So can you use it with what you have if if you're working for if you're an investor working from home, is this product going to be useful to you? Because those are the ones that are going to be where the growth is. If you're an investor with a cloud presence of some kind, can you use this on your cloud? Is it going to help protect your cloud if you can't use it and you're a reasonable size? Business is a pretty much a good chance that nobody else can either. Now, that doesn't mean there are going to be some niche technologies. There are some specific things that are technologies that will be sold to other people in the business. Think of it kind of like along the Dolby Labs model. There are companies that specialize in very, very niche things, like data feeds that are consumed by information technology, security companies. There are people who specialize in certain types of ASML that are tools that those of US building products for end user consumption used. But if they're selling an end user product, can you use it or can you find someone who does? And then obviously, can they give you more than one person who was willing to pay for it to use it?

Speaker1: [00:12:50.34] Right. Well, there are a lot of subsectors and applications within cybersecurity. He had to pick one or two to be at the top of the list for good media opportunity for investors to pursue. What do you put at the top of the list?

Speaker2: [00:13:01.42] Anything that enables digital transformation and cloud migration? I would say that that's that's probably the biggest thing that's finally happening. People have been talking about it for a long time. But the stuff that the workflows that have been moved to the cloud are still nascent, people moving real line of business stuff into cloud environments where they're accessed from anywhere. It's really a big secular thing. And I think the thing that probably will enable that is various technologies that enables zero trust networking.

Speaker1: [00:13:27.39] What about the new technologies out there, like autonomous vehicles and Iot devices where you have to provide security for that as well? Where are they on the application list, so to speak?

Speaker2: [00:13:38.31] Well, that's that's part of the whole digital transformation, right? This is securing anything anywhere, no matter what it's doing and whatever environment it's in, it is an autonomous vehicle is changing networks. It's on a cellular network. One minute it might connect to a Wi-Fi network. The next or maybe the phone that it's using for its navigation changes. You have to be able to secure that. And that's at any time anywhere. Protection profile, Iot. The thing about Iot is they're cheap and they're tiny. And the Iot vendors have zero incentive whatsoever to add to the capability or cost of those things. And in most cases, they're not configurable. So, again, you have to be able to secure them outside of the device somehow at the network level with what will most cases have to be services, because you're not going to control all the equipment, the network.

Speaker1: [00:14:26.70] Right. Well, you mentioned a moment ago that cybersecurity seems to be an afterthought for most things and is to be considered a nice to have, but it's now becoming a must have. What's what's going to drive people to actually put cybersecurity first and foremost? And the decision of building a product and deploying it is is that day upon us or is it still coming?

Speaker2: [00:14:45.51] I think it depends on the market where it's upon us and anything related to, for example, government contracting. The CMC rules now say it's it's not a an afterthought. It's got to be built in and you're going to see a lot more of that. And government is becoming a bigger part of the economy. So that's going to drive a lot of the product requirements for the type of things that people buy. I think also people are becoming far less tolerant of the endless drumbeat of having their data stolen and then as a result, having to lock down their credit reports, etc.. So I think people are going to start demanding more of it. You do see that more in the high end of the market. I think a lot of the people in the more consumer and the market are going to expect it from their service providers. And if they don't get it, they'll change service provider.

Speaker1: [00:15:36.81] You think we'll see a reengineering of the Internet itself to make it just fundamentally more secure? It seems like most of what we're doing is just plugging holes and the leaky boat,

Speaker2: [00:15:44.88] You know, Marcus, my socks, my Biola, everybody who I'm still very close to has said that for years. I think the problem, like anything else, is you've got such an embedded technology base that's switching at a wholesale is is really, really hard. I mean, how for how many years has this been coming? Right. And the rail gauge in large parts of the world is still dependent on the width of the Roman warhorses posterior. You know, I mean, any kind you get sufficiently embedded. And better technology, it's really hard to switch out. I think that also the reality is the Internet protocols themselves are flexible enough that you can layer a reasonable amount of security on top of it if you do it right. I think people overcomplicate the way they're doing it in many cases. But try to stop users DNS, which is ubiquitous. Everything good or bad on the Internet starts with the DNS query. Generally, it's a natural enforcement point.

Speaker1: [00:16:41.58] That's right. Well, in the last few minutes that we have here, what else should we care that we have it?

Speaker2: [00:16:44.88] I think the biggest thing to cover is how people go about looking at security. There's a lot of people chasing. The next bright, shiny object was UBA or architectures like Sasy, which Gartner is pushing right now without even looking at the most important fundamental basics. Right. You don't go adding an alarm to your house. If you talk, if your doors don't lock and your windows don't lock, you've got a sliding door. You can take a piece of wood dowling and stick in it at night. And that's a very effective way of securing the door. It forces them to break the window to get in. People spend quite a lot of time on intrusion detection, prevention systems and security, event management tools and threat intelligence to go admire the problem and create nice, pretty graphs. And and they buy from vendors that have big pupu maps that show, you know, this attack and that attack. They don't pay attention to the really basic stuff, such as did I make sure my firewall has the latest patch on it? Because there are ways that the VPN can be exploited or the software itself is insecure. Have I made sure that my rules make sense? Do I do some level of DNS filtering even if it's just forwarding all of my queries to Quad? Oh, are my vendors like my Web browser? Bypassing my security, because they're going to forward all my queries up to CloudFlare now instead of allowing my own security tools to inspect it, because with the combination of what they what they're calling DNS over https and auto, which is a better name for it, and quick, which essentially doesn't, will bypass approximating SSL.

Speaker2: [00:18:23.15] It's saying that whatever the the content delivery network decides is your security policy, is your security policy as opposed to the one that you want to enforce. So the other thing is, don't just randomly insert Trojan horse products into your network that are going to bypass all the where all the work you're doing. Be aware of what you're buying. Be aware of what you have run good inventories. And you know the basics also patch regularly. If there's a security patch out, don't wait a month to say, well, I must evaluate this in my lab to see if it causes me problems. Well, we've reached a point where the balance between a false positive or the patch causing you some problem is tilted far more in favor of. Yeah, but if you don't do it, you're going to get ransomware and you're not going to be able to use your network at all. It used to be, well, OK, like a lot like the Weird Al Yankovic song Virus Alert, where people kind of laughed at the hysteria that there was around forwarding all these. Well, there's a new virus out, too. This is real. People die because of ransomware, because they can't be admitted to a hospital. People use lose hundreds of millions of dollars because they have to rebuild their entire network. So I think that the other thing is that people have to realize that there is some level of inconvenience in being actually secure. And and accept that

Speaker1: [00:19:48.15] That's a good point. Well, how best for listeners get back in touch with you.

Speaker2: [00:19:51.71] So we have a website at Dot.com. I have a LinkedIn page. Quite happy to post on it fairly regularly. I'm not that active on Twitter, but our marketing department is. And the best way to reach me personally is to send me an email to OMB at Threat Stop Dotcom. I answer email was great.

Speaker1: [00:20:10.82] Well, put that in the show notes. I want to thank you for joining us today and hope to have you back for a follow up soon.

Speaker2: [00:20:15.29] Thanks very much.

Speaker3: [00:20:17.83] Investor Connect helps investors interested in startup funding. In this podcast series Experience, investors share their experience and advice. You can learn more at Investor Connect, Doug. Paul Martin is the director of investor Canek, which is a five Wannsee three non-profit dedicated to the education of investors for early stage funding. All opinions expressed by Hall and podcast guests are solely their own opinions and do not reflect the opinion of Investor Connect. This podcast is for informational purposes only and should not be relied upon as a basis for investment decisions.