"We're having to be much more aware of threat modeling and risk assessment. Before it was just like, 'Oh, somebody told me this is the product I need to use. Go. Put this on my machine and will detect all the things and all will be great.' Whereas now for companies and for individuals, having just one layer of security really isn't enough."

MARCH 9, 2020

Fast-Moving Threat Models

Presenter: Lysa Myers

Summary

Threat models have grown to enormous complexity since the boot virus days and show no signs of slowing down. How does this affect cybersecurity at the workplace and at home? Brian talks with Lysa Myers, Security Researcher at ESET, and gets her take on adapting research, tools, and specialization to keep up with the fast pace.

Transcript

Brian Contos:

Welcome to the Cybersecurity, Effectiveness Podcast sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve and communicate security effectiveness. I'm your host Brian Contos and we've got a really special guest today. Joining me is Lysa Myers. Welcome to the podcast, Lysa.

Lysa Myers:

Thanks Brian. It's great to be here. Thank you for having me.

Brian Contos:

Oh, it's my pleasure. And you know, Lysa, I have a lot of things I want to get to, but before we get started I'd love it if you could give our listeners a little bit of background about yourself, the path that you took that led you into cyber and what exactly it is you do today.

Lysa Myers:

Well, my path was kind of an unusual one, which was facilitated somewhat by coming in during the dot com boom. I was a florist for a number of years and was intending to go to school as a landscape architect. I got wait listed for that degree program and realized that I really just needed to work and make money to live. And so, after a few years as a florist, where work is very seasonal and you kind of get laid off at least once a year, I decided to take a job as a receptionist at a security company. And I would do odd jobs for that off and on as I had time. Because, being a receptionist you have a lot of downtime and they had a lot of need for extra help. Especially, this is when viruses started to become a big deal and make the nightly news like Melissa virus.

Lysa Myers:

And so, flash forward 10 years, I was the one who was teaching new virus researchers. I basically spent that 10 years asking a lot of questions and doing the grunt work that nobody else wanted to do, of organizing things, and making customers feel comfortable, and soothe in their time of need as they're sending us samples. So that allowed me to get that on the job experience over a good long while. But then, part of my day to day duties, they started a blog for the company I was working for in the virus research department and I was one of the first people who volunteered for that. And I really enjoyed it. And I started talking a lot about testing of security products. And from there somebody read those blogs and went, "Hey, this person has good ideas about testing," and hired me to do third party testing. And then from there just has spiraled out so where I'm spending more time writing and spending more time advising people and educating people about how to protect themselves.

Brian Contos:

I love it. I love it. It's so interesting to me when I hear how people get into this space. I think you're the first one that has gone from florist, but I've had a number of other very unique things as well. And I love that about cybersecurity because not everybody follows that traditional, maybe computer science, mathematics type background. I think that's a positive thing for our industry. So you mentioned briefly, you spend a lot of time advising and educating and you've been on the forefront of this for a while. How have security careers themselves, how have they changed from when you got started in all this?

Lysa Myers:

It's been an interesting evolution. A lot of people started as hobbyists, because there wasn't really a degree program that covered this sort of thing. There was a lot of people who transitioned from military and learned networking and went into network specialization or they were assist admins and they went into help desk or virus cleaning services. That sort of thing. So, job titles started out really amorphous and you had to do everything. And then, we're getting into this area of specialization. Like, you're a defender or you're... I guess the red team, blue team idea. And now we're seeing quite a bit of shift towards recognizing that there are a lot of careers that are security specialists because what we do is so different.

Lysa Myers:

Being a marketing person for a security company and doing it well is a very different thing from being a marketing person in any other industry. The way you have to behave and the things that you have to focus on is vastly different. I recently saw a color wheel where it was like red team, blue team, green team, orange team, whatever. And, while that was kind of confusing, because I think I'd be somewhere like rust team. Because I'm a little bit blue, a little bit orange. The idea that there are a variety, there's a whole rainbow of different security specializations. And we really do need people in all of those specializations.

Brian Contos:

And I know a lot of your career has been on the research side. Maybe we could dig in specifically to how has research changed and maybe some of the tools and threats and specialization there?

Lysa Myers:

Yeah. When I started it was, I mean, we were exiting the boot virus days. So, viruses were a teeny tiny and there was contests to see who could make the smallest malware. And within that time period there was also the addition of the difference between virus and malware because some programs didn't necessarily detect trojans. And then from there we got into grayware. Where you've got potentially legitimate software that's behaving really badly or something that network administrators wouldn't necessarily want on a corporate network that they want to be alerted about. So we had to make all these decisions about, are we just detecting viruses or we detecting malware? Most companies, well I think any company that still exists, is detecting both malware and viruses. Especially because malware is the much bigger threat now. And then, a lot of companies also have the ability to detect the grayware. The stuff that's you wouldn't necessarily want on your network or that people in vulnerable situations really don't want to... They want to have detected, they don't want to have on their computer.

Brian Contos:

So, let's go into the actual security threats then. You mentioned viruses and malware and some of the different things and then how the stakes have changed there. But how have security threats actually changed throughout this process?

Lysa Myers:

In the beginning days it was much more simplistic and there was a lot easier for virus researchers to actually look at the file and since it was usually code as text, basically. You could see very clearly what it was doing. And in the last decade or so, things have gotten much more complex. They tend to come as static malware where it's an executable file or it's a file-less malware. Or someway it has made it much more difficult for someone to figure out what's going on. Because in the early days it was about getting a notoriety for doing something really cool. Or "cool." Versus now it's about staying under the radar for as long as possible. And it's been interesting to me to see how things have shifted on both sides.

Lysa Myers:

Like, the complexity and the malware side, but there's also the complexity on the research side. Where, back in my early days, it was very much a hands-on process. You physically take the sample and look through the code and see how it goes. But now there's a lot more of that that's being done automatically by machine learning and neural networks where it's looking through the file and finding characteristics going, "Okay, this is fishy looking. Human look at this more," or "This is clearly fishy and add this as a provisional detection."

Brian Contos:

I'm wondering if we take everything you've talked about into consideration, the changing threats, how research has changed, the disparate careers now in the space. When you boil this down, how does this really affect the threat model you think, for businesses and maybe even the average user at home?

Lysa Myers:

I think we're having to be much more aware of threat modeling and risk assessment. Before it was just like, “Oh, somebody told me this is the product I need to use. Go. Put this on my machine and will detect all the things and all will be great.” And, that idea had its problems from the outset, but for most people that was enough. Whereas now for companies and for individuals, having just one layer of security really isn't enough. You need to have security software, whatever that means for your computer or organization. Plus you need to have multifactor authentication and maybe having a firewall and a variety of things. How much that has changed over the years has surprised me.

There are certain things that 10, 20 years ago I was like, "Oh, that'll never be acceptable." But people using Tour, that was a thing that really shocked me. For most people that's just too slow and too cumbersome. Or freezing your credit. That's another thing that I never used to recommend that because no one's going to do it. But now, that's the default position and it seems like-

Brian Contos:

Oh God, after the latest breach freezing the credit, I had to get on the phone with my parents, and my nieces, and my nephews, and my cousin. And I think it was... Was it Stephen Colbert who did actually a really good piece on that? I think. "It might've been Stephen Colbert" I was like, "sending this video link out saying just watch this and then this is how you contact..." I said, "Whatever you do, don't lose the password when you freeze it."

Lysa Myers:

Oh God.

Brian Contos:

So, that one hit close to home.

Lysa Myers:

I mean that's a good point too, is that threat modeling for home. Security people have laughed forever about password books, but if you have someone in your house who's not real tech savvy and for whom password managers is just too much to deal with, writing passwords down in a book may really be a viable option in the whole, "Change your passwords every 90 days." Now they're saying, "Yeah, maybe not. If you have a good password, just keep that until it becomes breached" or whatever.

Brian Contos:

Just wait until you get that notification that "you've been pwned."

Lysa Myers:

Exactly.

Brian Contos:

And then use that as your indicator that now it's time to change. It is funny how they've matured over the years. And I do... on Reddit, if you use Reddit, and you follow the cybersecurity you always see these, "Hey look, I found a password management book in a bookstore." And they're just like, "It's half used already."

Lysa Myers:

Oh God.

Brian Contos:

So let's talk about has the public, and I guess when I say that what I'm really asking you is about the executive team, but have attitudes changed towards cybersecurity in your perspective, from any of these different angles?

Lysa Myers:

It's starting to. I think very much in the early days, trying to get executive buy-in was like trying to pull teeth. Just trying to justify something that was so expensive, it was like climbing the highest mountain. But as we're seeing more and more companies having issues like, there was recently the Capital One breach, they're saying, "Security team warned about this thing and they were ignored." And if you think about the costs of repairing the damage versus they asked for half of that money.

Lysa Myers:

For some reason, I don't remember if it was the Capital One breach or another breach, but it was like, "It's $80 million. Had the security team asked for $40 million, they would have been laughed out the door." But, it would've saved them half the cost of repairing the problem. And you're starting to see more companies going, "Okay, we have to be compliant with X, Y, or Z regulations" or the whole alphabet soup as it were, of regulations. So that's part of it.

But also seeing so many other companies just getting hammered because of breaches. And on more down to earth levels, like understanding that education is such a huge part of this. It's like, you can't teach calculus in a day. You can't teach security in a day. You need to do little bitty bits and keep doing it. Build on whatever forever. Not just one and done.

Brian Contos:

That's a good analogy, actually. It's interesting because today if you go to YouTube and you do a search on, I don't know, CEO cybersecurity, you'll see there's a lot of CEO's even for power and energy. Which people don't generally think of as the forefront of cybersecurity, visionary thought. CEO's of these companies that are doing videos about their commitment to cybersecurity, and why it's important, and they're talking to the media about it. And it has nothing to do with, one day they woke up and they felt that cybersecurity was important and they needed to pay attention to it and they wanted to do the right thing. Those things might've played a small part, maybe. They're doing it because they're stakeholders are saying this is a material risk right up there with earthquake or a terrorist act or the economy or anything else in between that could have a material impact on our organization. And because it could have a material impact, it better be understood and communicated at the highest levels of the organization.

Brian Contos:

So, I'm glad to see that because I think cybersecurity for a long time, has been almost a grassroots movement. It's been this bottom up. And I think people like you have helped fill that gap and get it to the point where, now it's bottom up. But it's also top down. It's also side to side. So it's really hitting its stride, if you will. And that just didn't happen by accident. That happened through people constantly spreading the word and through education and advisement work and awareness and things like that. It's not over, but boy, we're in a much better place than we were even just a few years ago. And I guarantee you, you would not have seen anybody from a CEO of a power and energy company talking on YouTube about the importance of cybersecurity, right. So I think it's a sign of the times, if you will.

Lysa Myers:

Absolutely. I think a lot of companies are realizing that it can really be a business differentiator. They can make more money if they are loud about how seriously they take security.

Brian Contos:

So let's talk about the industry itself and more specifically attitudes. Do you think that attitudes or perspectives have actually changed in our industry?

Lysa Myers:

That I think is beginning to change as well. I remember once upon a time that it was the going phrase was, "You can't patch stupid." But you can't expect the general public to understand the inner workings of a car if they've never been trained on using a car. Same with computers, if computer security is telling people to do things that are unintuitive, computers are designed like, you click links in the email because they're highlighted and available and you're telling people to not do the thing that the computer is telling them that they should do.

Lysa Myers:

So the expectation that people are going to intuitively understand all of this complicated stuff, which is kind of ridiculous. But it goes to usability and being aware of accessibility because security can be a challenge for a lot of different groups like lower income and domestic violence situations where you have to overcome a huge hurdle to do the secure thing. And people are starting to understand that the way computers are designed right now, the way softwares are designed right now is meant to make it easy for security problems to happen and we need to design differently in order to change that.

Brian Contos:

I love that. I've never heard it phrased like that, but I think that's probably the best I've ever heard it put. I mean essentially, it's designed for maximum usability, right?

Lysa Myers:

Yeah, exactly.

Brian Contos:

And whether the intention is... they're good intentions or they're nefarious. It's designed for maximum usability. So, it takes advantage of that. That's a very interesting way of putting it. Well, Lysa, as we wrap up here, who is your favorite superhero or super villain and why?

Lysa Myers:

So, my choice on this one is probably a little nonstandard as well. Have you ever watched the Steven Universe cartoon?

Brian Contos:

No, I haven't.

Lysa Myers:

So, it's absolutely delightful if you want your faith in humanity restored. It's a great watch. But Amethyst is my absolute favorite. She's not a traditional superhero, and a lot of ways, she's not at all what a hero's expected to be. She's crass and gross and really casual. And she doesn't really fit the mold--

Brian Contos:

Oh, I like her already.

Lysa Myers:

--that she’s supposed to be. But whether she's alone or whether she's working together with others, she's creative and passionate and she kicks a lot of butts, so.

Brian Contos:

I love it. I'm going to check that out. Well, thank you, Lysa, and thanks to all our listeners for joining and be sure to check out other Cybersecurity Effectiveness Podcasts sponsored by Verodin.