Micro Focus Reimagining Cyber Episode #39 Raveed Laeb

Fri, 9/2 9:58AM • 23:37

SUMMARY KEYWORDS

cybercrime, cyber criminals, business, organizations, people, services, attackers, happening, legitimate, cyber, ecosystem, work, cybercriminals, credentials, ransomware, security, malware, actor, commodity malware, industry

SPEAKERS

Rob Aragao, Stan Wisseman, Raveed Laeb

Read | Listen

Raveed Laeb 00:00
Oh five years ago, 10 years ago, we were a cyber criminal and had a revenue model that relied on you gaining access to, let's say, CEOs, emails in companies, you had to know to do a lot of stuff. You had to find ways to not appear suspicious. In today's cybercrime economy, you don't really need to do anything. Rather than just buy services from people, you go into an automated shop, and that's it. It really outsources everything that you needed to do before.

Rob Aragao 00:35
Welcome to the Reimagining Cyber podcast where we are short and to the point perspectives on the cyber landscape. It's all about engaging yet casual conversations and what organizations are doing to reimagine their cyber programs while ensuring their business objectives are top priority. With my cohost, Stan Wisseman, Head of Security Strategist, I'm Rob Aragao, Chief Security Strategist, and this is Reimagining Cyber. So Stan, who do we have joining us for this episode?

Stan Wisseman 01:01
Rob, our guest today is Raveed Laeb. Raveed started in Israel's defense forces military intelligence and has served for around six years in a variety of different intelligence outfits. After he left the military Raveed started at KELA as an intelligence analyst and team leader moving through sales and solutions engineering and and now he is the VP of Products at KELA. He is, I want to know, still, a captain in the Israeli reserves revealed is great to have you with us today is going to be a very interesting topic, I think, for our listeners. Raveed, anything else you want to share with your background before we get started?

Raveed Laeb 01:36

Thank you, Rob. Thank you, Stan. Great to be here. No, nothing super specific. I think that, as you've mentioned, like a lot of other people in the industry, I got my head start in the military doing intelligence than have pivoted through everything from social engineering, intelligence, and everything that's in between. I think that, like a lot of other people, probably in the same space. I don't come from the more classic kind of IT security engineering background. I think that we stood out a lot in the industry, so I'm no exception to that.

Stan Wisseman 02:11
Well, given your your your background and your ability to understand the the the cybercrime kind of ecosystem, we, that's where we want to delve in with you and explore that that world. You also are coming in from a white hat perspective, which is a good thing to have. So this ecosystem has evolved rapidly over the last few years. And it's, it's causing a lot of pain for a lot of organizations, whether it be in the government side, whether it be in industry, everybody is touched by the cybercriminals. And the victims are many times powerless. And I don't think we have a very good understanding of really what's going on. As far as this, this whole parallel economy that's kind of obscure from most of us, can you shed some light and sort of like explain the current state of this ecosystem and how it works?

Raveed Laeb 03:10
Of course, then, so I think the key phrase that you've mentioned, is economy, because I think that sometimes, most definitely in mainstream media, but a lot of times in places even where like professionals have to understand what's happening in terms of the threat landscape. It's hard. It's easy to think about cybercrime as this shadowy, weird kind of thing, kind of a Wild West happening in the background of everything, a chaotic and weird and lawless place. Whereas, in reality, just like a legitimate business, cybercrime works on, or at least most cybercrime, works on money. So cyber criminals want to make money. They want to monetize the goods and services that they have to offer. And just like legitimate business, in the real world, things happen within that economy that we also see reflected in usual businesses. Things like specialization. So different people taking different skill sets, and understanding how to monetize them, how to use them, how to increase the return on investment, so they can just have better business and keep more money for themselves. And also a lot like legitimate business, cybercriminals are very much worried about scale. They are worried about having the same thing be repeatable in terms of business success, and over time, that really drives the economy into a few different or very distinct places. And I think that some of them, or at least the things that we see, and feel their impact in the real world, like ransomware. They tend to be, or tend to become, very prominent. And just like the internet as a thing has become very prominent, or just like Netflix and Spotify have become winning products or - that's exactly what happened for ransomware. For example, it's just threat actors that had success, found key principles that they need to make it repeatable, and then just make it work. And also a lot like legitimate businesses, cybercrime relies heavily on supply chain. It relies heavily on having different people to which you can outsource things that you might not be able to do yourselves. So, for example, a lot of people like to think about the golden age of startups, right, having Mark Zuckerberg in a garage somewhere, making all the Facebook happen with two different people on one computer. Everyone doing everything, doing marketing to encoding, doing customer success. And as the business grows, you can't really have that. You need, you need to have coders to do the coding, you need to have customer success, people to do customer success. And that is exactly what we see happening in cybercrime. People understand their

niches, understand their roles, understand how they can contribute to the business, and really find their places. They find ways and channels to offer what they have to offer goods and services and everything in between. And they find ways to cooperate with one another, forming collectives, forming even a lot of times actual legitimate businesses as kind of fake companies through which they can actually make things work. And really find ways to be innovative, beat the market, and succeed in what they're trying to do.

Rob Aragao 06:37
Raveed, let's dive into the business aspect of it, because I think you call that a very important element here, which is, many people kind of look at the surface level of when they see some sort of breach occurring, the different impacts, they don't realize, as you're calling out, it's a real business, right? Cybercrime has grown tremendously over the past several years. And when you think about that, you mentioned ransomware as a service, isn't is another example of areas of specialization, right? People are putting out their capabilities for sale, they're looking to get into environments to be able to get their hands on data, so they can go and monetize the data, right? So, there's all these different levels of sophistication that has been kind of evolving over time, right, for cybercrime, and that cyber criminal aspect. What are some of the different kinds of examples you can call out that you've seen as part of the evolution over the past few years?

Raveed Laeb 07:26
So, I think that something that is very interesting, and there's a lot of talk in the industry about it, is how commodity malware, so, simple malware, nothing too sophisticated, nothing like nothing that's been produced by a nation state and can and use zero days to spread, but really simple malware that you can catch on the internet, just like you catch the common cold, how is that being used by cybercriminals? For a lot of years, or for a very long period of time, at least, defenders, enterprises, corporations, like big organizations tended to look at commodity malware infections as something that happens that isn't a big deal. However, what we really see lately, in the past two or three years probably, is how commodity malware, the same thing that it was seven, eight, ten years ago, is now becoming a staple in the, what some organizations call ‘big game hunting’. So ransomware as a service that targets big organizations. Think about that works good. Let's take a scenario: someone is now infected with commodity malware, or, or the type of malware that's most commonly referred to right now as an info stealer. And what that specific type of malware does is it just grabs into a computer, pushes itself in, grabs all of the passwords that you can find. So, passwords that are saved in the browser, saved in different clients. And then it just dissipates, it dies, and it does nothing else. After all of the credentials have been sent to attackers. A lot of defenders, if you were to talk to them maybe four or five years ago, they would say that, yeah, it's not, it's not a threat. It's not persistent. I don't have a breach right now. However, what we see right now, that is more commonly happening, even more so from the beginning of COVID, when a lot of people are working from home, is that personal computers or computers that are out of the actual network can be used to login into system critical resources. So, you can have an employee being infected, and credentials with session cookies and a lot of very sensitive things that are used to login into an enterprise VPN are now at the hands of cybercriminals. And really, when you think about an info stealer, you can think about the many different things that that people can do with credentials. Someone can break into your computer, still have your all of your credentials and just use them to start to set your Spotify or Netflix account. On the cybercrime

ecosystem for two bucks, they can use it to gain access to business emails, and sell that for a few hundreds of dollars. Or they can use that to log into enterprise VPNs and sell that on the cybercrime ecosystem for thousands of dollars. And we see that specific thing being very prominent right now with what we call or what the industry tracks as initial access brokers. So, a specific type of actor that specializes in obtaining these first few breadcrumbs of accessing a network, even from very simplistic means, like commodity malware and info stealers, leveraging that and then selling that for thousands of dollars. And that really becomes the foothold in a lot of actual destructive, sophisticated, quote-unquote, 'ransomware attacks' that we've seen. And really, maybe the bottom line here is that a simple or seemingly simple threat, like an info stealer, sitting for five minutes on a computer, stealing passwords, and then disappearing, while not being super critical five years ago, today, it's something that organizations should look into very thoughtfully, because in that ecosystem, where the first person gaining into access into a network is not necessarily the one monetizing it and credentials and network access passed from hand to hand, you never know where something that started in your environment ends. And that is a very major shift that we've been seeing. It's stealing credentials for maturing them, grooming them, selling them to sophisticated actors, and facilitating wide, large attacks that have actual impact on on all of our lives.

Stan Wisseman 11:49
Another example you've written about Raveed is the whole servitization process, just like legitimate businesses, right? There's, there's this process that is repeatable, and you provide that as a service. And we mentioned ransomware, as a service, is that trend going to accelerate?

Raveed Laeb 12:09
So personally, I would very much say that it would. And again, probably following the path of, as I've probably said, too many times, legitimate business. We, as private consumers, are consuming more and more things as a service. So, most of the products that we use on the Internet are not actual software clients that we buy, like we did 10-15 years ago, we use everything as software as a service. Instead of going and renting DVDs, we stream them as a service via Netflix, exactly the same thing is happening with cyber criminals. So, going back maybe to that startup example, five years ago, ten years ago, you were a cyber criminal and you wanted for some reason, you had a revenue model that relied on you gaining access to to, let's say, CEOs, emails in companies, you had to know how to do a lot of stuff. You needed to find a creative ways to obtain email credentials, so you can get in. That is more complicated than it might sound. Say, for example, that your revenue model relied on business email compromise, where you try to extract money from the organization via wire transfers. Then you had to speak the same language as the person you're trying to defraud, you had to find ways to not appear suspicious, and you kind of either had to do all of that yourself, or be a part of a conglomerate of an organization with a lot of different people who can help you with it. In today's cybercrime economy, you don't really need to do anything. Rather than just buy services from people, you go into an automated shop, which we know of a lot of these right now, in the cybercrime ecosystem, you get an invite, you log in, and then you have a shop where you can actually buy for $50, $100, $150, access to business emails, of corporates of governments, of very big organizations. And that's it, really outsourced everything that you needed to do before. In order to gain that access, you just go and buy it from someone who specializes in that. Then again, let's go with the wire transfer example. You need to use proper standardized English to not appear suspicious. You can very easily find right now in the

cybercrime ecosystem, translators offering their services for anything that requires business-level English, for example. So, you really don't need to know a whole lot yourself because you can just use different services. So, we've been seeing that more and more and I really do think that it will become even probably even more prominent as time goes on.

Rob Aragao 14:58
I didn't even think of that - the translation services. It makes sense. Because of the examples we were just talking about right. Here, hey, so Raveed, let's go into, right, the legitimate business aspect of things. So as they're operating their business models, right, and they're looking at different opportunities, leveraging services, as we've been talking about what we're seeing, obviously, in kind of the, you know, aspect of the way organizations are operating, there's a lot of demand for how do we become much more efficient? How do we do things from an automation perspective? How can we leverage AI and machine learning? What are you seeing in that realm as it relates to these cyber kind of enterprises that are out there?

Raveed Laeb 15:38
We've had a lot of insight into the inner workings of cybercrime business. Just a few months ago, or early 2022, I believe it was where the country group had a lot of their messages leaked by a security researcher. And that really showed maybe just to stress to your point, a lot of the struggles that cybercriminals have, as well, with finding people to work for them with having these people have enough knowledge of technology, and being able to automate simple tasks so they can be efficient in the work. We can see a lot of discussions about how much they get paid, for example, and where are the offices are located. And that was a very interesting point that showed, for example, how do they communicate. They want very easy chats so they can communicate efficiently between one another. They want scripts and tools that automate their initial accesses that they want to validate for them. So, they don't, so they don't have to do a lot of manual work. And they think that we see probably two major things happening here, I would say, the first one is cybercriminals erecting businesses that are based on automation. So, say, for example, five years ago, again, you had credentials that you wanted to sell, what you would do as an attacker, you would go on the community on the forum, and you would post, I have something for sale, please contact me so I can sell it to you. What you do right now is you sign up as a seller, even online automated market, upload your wares there, where people just buy them. Without doing anything with paying via cryptocurrency to the website, you don't have to lift the finger. So, one thing that we're seeing is cyber criminals taking their businesses and their own technology that they are building into that realm. The second thing that we're seeing is cyber criminals using legitimate software, and legitimate tools that regular organizations use to make their work easier as well. But I wouldn't name any names right now, but a lot of legitimate popular services, scan the internet for vulnerabilities for exposed technologies, and make that data available for security researchers for defenders to understand how their perimeter and how their organization looks. So, you have legitimate services that do that, for good purposes. We are. And maybe even before a lot of defenders, attackers have gotten wind of that as well. So, we see a lot of attackers that try to use legitimate services, security services, services, security tools, automation tools to make their work easier. And just another example from the country leaks. In the leaks, you could see the actors talk about trying to purchase security products from security vendors, so they can really understand how these products work, how to leverage them and how to exploit them on the other end as well. So, I think that in terms of

automation, in terms of leveraging services and products that use cutting-edge technology, I probably wouldn't say that we see cybercriminals doing that themselves. Like I wouldn't say that we see cybercriminals building ML or AI-based software for their own use. But we sure do see them abusing legitimate software, that actual good, legitimate vendors sell on the market. And we do see them heavily focused on automation, when it comes to how they manage their own businesses, if that makes sense.

Stan Wisseman 19:25
It does make sense and unfortunately, you've reinforced our belief that organizations have to assume they're gonna have impactful cybersecurity kind of incidents and breaches, given this maturity and ecosystem, right. And I guess, if you look at the defensive side of the equation, how can organizations become more resilient in the face of this very efficient, increasingly evolving, legitimate, like, you know, cyber-criminal ecosystem?

Raveed Laeb 19:57
So that's probably the trillion-dollar question, isn't it? So as mentioned in the beginning, I don't come from an IT security background. So, I'm not probably the best persona to talk about what you should do better. Specifically, technically, what I can say is that most of the time, the stuff that organizations need to do is the stuff that they already know that they need to do to understand the patching cadence that you need for your technology to make sure that you're ahead of critical vulnerabilities, and force multi-factor authentication on everything, everyone, anywhere, every time, or anytime. Really, you don't have to reinvent the wheel, at least, you need to understand what's the critical things that you should pay more attention to, and the things that you should protect in a much more excessive manner. And the key to doing that is understanding what bad people do in the real world. Because I think that the key thing to that whole industry, again, just like legitimate businesses, is that cybercriminals and attackers in general, are more more than everything. The report to Mystic, everyone likes low-hanging fruit, you kind of have to assume or that that's the mentality that cybercriminals are not necessarily actively going after you. They're going after everyone, if you happen to be the one that they see right now. That's the issue. So limiting or reducing your digital footprint, the attack surface that attackers can see on you the opportunities that they have to get in your network. That's key. There's a cliche that a lot of people like to mention, or at least I personally think it's a cliche, where attackers need to be correct only once, and defenders need to be correct 100% of the time, and that's like kind of a built-in estimate tree. I don't necessarily agree with that. I think that that's overly simplistic because the key to, or one of the keys, at least, to trying to have good security is security in depth, a threat actor shouldn't need just one opportunity to get into your network, they shouldn't, they should get one opportunity for every layer of defense that you have, if you just have an EDR. And that's it. And all that a threat actor needs to do is to bypass that EDR. That's an issue. But if you have a segregated network as well, and you have multi-factor authentication, then the threat actor needs to be right three times in a row. And not just one. And statistically, that is much, much, much, much better.

Rob Aragao 22:39
Raveed, you came on you shared so much great information, especially as relates to evolution right as what we're seeing out there. What you're seeing out there around cybercrime, and the reality that it truly is a business behind the scenes that is operating now with many different services available, much

easier, right to get out there and do some serious damage. So, thank you for coming on and sharing your experiences and what you're seeing out there.

Raveed Laeb 23:00
Thank you so much. It was a pleasure. Thank you, Rob. Thank you, Stan.

Stan Wisseman
Hey, thanks for being here.

Rob Aragao 23:05
Thank you. Thanks for listening to the Reimagining Cyber podcast. We hope you enjoy this episode. If you would like to have us cover a specific topic of interest, feel free to reach out to us and you can find out how in the show notes, and don't forget to subscribe. This podcast was brought to you by Reimagining Cyber, a Micro Focus line of business, where our mission is to deliver cyber resilience by engaging people, process, and technology to protect, detect and evolve.