NETEVENTS GLOBAL IT SUMMIT

SAN JOSE, USA

OCTOBER 3 & 4, 2019

FINAL

Keynote Panel Session:

The Dark Web: Fight Black to Protect Your Networks and Data

Introduced & chaired by: Vikram Phatak, Founder, NSS Labs

Panellists:

Ted Ross	CEO & Founder, SpyCloud
Thomas Edwards	Special Agent in Charge at U.S. Secret Service, San Francisco
Jan Guldentops	'White Hat' Hacker

Manek Dubash, NetEvents

Okay, thank you very much for an entertaining and illuminating presentation, thanks Ted. Okay, let's have the next panel down. It's Vik Phatak from NSS. Vik, where are you, and his panel please. There he is, come on down and the panel please.

Vik Phatak, NSS Labs

So Ted, that was interesting and I'm sure terrifying for some folks.

Ted Ross, SpyCloud

I did my job.

Vik Phatak, NSS Labs

Yes, right. So we're doing a bunch of questions but generally your presentation blew the hell out of most of them. You answered them already. So I'll do a quick review on a couple of things and then we can move to some, I hope, to more advanced questions. How many companies - this is for Ted, I guess and then historic. So how many companies actually know what's out there on the dark web? How much of their information is out there?

Ted Ross, SpyCloud

When we go into a new opportunity and they haven't heard of us before and we show them their information, they're almost always surprised. So I would think that a surprising, a shockingly low number would realise how big this problem is and that their credentials are actually out there.

Vik Phatak, NSS Labs

So from obviously secret service, you're dealing with this all the time, right? Obviously with Ted's thing he goes in, people don't know, but you go to larger companies, is that still true? I'm assuming the threshold for you to get involved is fairly how.

Thomas Edwards, U.S. Secret Service

Yes, we know we will get a call from a victim company and we will start looking at what the actual loss is. There are certain prosecutorial guidelines as far as the amount of loss per judicial district in the US. Typically, it's anywhere from $250,000 to $500,000 for a prosecution, but it doesn't prevent us from doing the investigation. So we'll work with the company to try to remediate the loss, patch up the networks and stop them bleeding.

Ted Ross, SpyCloud

I do want to add one more thing, Vik and that is the larger the company they know their credentials are out there, but they've underestimated the power of that data until they see it.

Vik Phatak, NSS Labs

Okay, that makes sense. I know until I saw it, the light bulbs went off.

Panel Speaker - Male

The problem is you can monetise credit card data, you can monetise wire transfers, but to Ted's point, you don't know the value of those credential on the dark web and what it's going to cost the company to remediate the losses, whether it's through replacing their servers, replacing their infrastructure. That could be in the tens of millions of dollars. That's never accounted for when you're looking at prosecution, but it's an actual cost to the business.

Panel Speaker - Male

So what's the end game? Pretend I'm a bad guy for a second and I steal a bunch of credentials. Is it to try and get the money transfer from wire - wire transfer from a title company type of scenario? Or is it more - is that always the end game, or is there something else people are after?

Panel Speaker - Male

It depends on who's doing it. A good hacker hides himself and stays around for years at a time. We had a breach at [BODA] Conference, they were in there for five years before they were detected.

Vik Phatak, NSS Labs

But I mean if the primary motive is financial, how are they making their money?

Panel Speaker - Male

Well it depends, it really depends. There are so many ways of doing this. I had a case in a certain Antwerp sector that transfers a lot of small stones and it's more afraid from the tax collector than from criminals mainly. There they basically stole - they basically intercepted an illegal transport of blood diamonds, that's how they get away with it. They had it out of a mill account, they hacked a mill account. It's so many different ways of cashing in. We always see the simple ones with credit card data, but there are so many creative ways of doing this, it's incredible.

Panel Speaker - Male

I do think though that it's very common for them to put the money into an account where they can take that money and move it to many other banks quickly, so that they can basically launder the money. Move it around faster than the investigators can keep up. There's always the simple way of monetising and that's to get somebody to buy you gift cards. But hopefully the people at Best Buy now and Apple will realise why are you buying 1000 gift cards and look at the email and stop them from doing that. The big losses are typically wire transfers out.

Panel Speaker - Male

It's follow the money.

Panel Speaker - Male

To Ted's point, the organisations have become so sophisticated through the use of encrypted messenger apps, such as Telegram, or they can coordinate their attacks or their cash outs very quickly around the globe. So you can have a crew in Asia, a crew in Europe, a crew in South America, a crew in North America and when you want to cash out on any one of these schemes, whether that's credit card or bank wire, they can just send that message out to the network and it's instantaneous. The coordination is fantastic at the criminal level to take advantage of these vulnerabilities that are exploited.

Panel Speaker - Male

Once you know your information's on the dark web, which I'm assuming everybody's is at this point, so proactively in the future you get a password manager, but is there anything you can do to clean it up, like cleaning up a credit report?

Panel Speaker - Male

Yes, how easy is it to change your social security number? It's very difficult, right? So I think that we live in a world where you just have to know your data's out there and freeze your credit reports and when somebody tries to open up a new account, hopefully they'll have to actually call you to get approval to unfreeze it. It all goes back to zero trust. Your data's definitely out there. I know my social security and my date of birth were leaked as part of Equifax, because two months later new accounts were set up with my social security number for the first time ever. In 50 years, first time ever after Equifax. So there's a seven year fraud alert on my social security number now.

Panel Speaker - Male

I had somebody in Detroit take out a $28,000 loan from one of those short-term lender things and all of a sudden, they started giving me a call. Okay, so we just talked about social security, but what other information is out there? I hear medical records are hot, why would somebody want your medical records?

Panel Speaker - Male

We're seeing more and more, as they move industries and monetise this information, private health information can be used for a lot of different reasons, especially as governments provide more and more healthcare. You can use somebody else's information to get that surgery or that procedure. But also, you can think about it, if you get the information of a politician or a high profile individual and you have that data, you can use it to exploit that person and extort information. So it becomes really dangerous. Your private health data can be a treasure trove for organised crime.

Panel Speaker - Male

We were talking about privacy earlier and how in Europe there's a different perspective on privately, compared to the US. I've got an eight-year-old son, he has no expectation of privacy. But it sounds like if the bad guys already have our data, then we're not going

to have privacy anyway, right? We can't trust that it's not going to be used against us in some way, or am I misreading that?

Jan Guldentops

The thing is it's not because you have astringent privacy law in Europe that there's no data being leaked. Not much has changed in GDPR, everybody's scared for the fines, but the big breaches are still coming along. So it's going to keep on happening for a long time and there is no solution for that. Once your data is out there it's game over. Once you're blackmailable it's game over. There's no way back.

Panel Speaker - Male

What I'm getting at is it used to be in the US years and years ago that if you were gay or if you were something like that and you didn't come out, that could be used to blackmail you. Which is why everybody now, if they're gay, they come out, it's not a big deal, but in the 1950s in the US that wasn't the case. It sounds like if there's other things like that, that you have some medical procedure or something, you might as well let your colleagues know and folks know because otherwise it could be used against you.

Panel Speaker - Male

I look at it a little bit differently. You say it's game over and I say it's just the way things are. We have to live in that world now and just be - you have to accept it.

Panel Speaker - Male

The trick is, as a human right you have the right to keep certain things private, right?

Panel Speaker - Male

Yes, criminals don't care about that and they've already set the stage. So now we live in this world and we just have to deal with the world we live in. I think trying to undo that is just unrealistic at this point.

Panel Speaker - Male

I agree with that, it's going to be very difficult, but we need to find a way to keep our privacy, because it's a basic human right. You should know…

Panel Speaker - Male

I agree with the spirit behind GDPR, by the way, too.

Panel Speaker - Male

Yes, you should not know everything about me before you step onto a panel, because you can do a query somewhere. We have a generation coming along now who have the idea that they're never going to have privacy, everything's going to be public. That's a

bit of a sad way of living, isn't it? If you meet somebody and you can look them up before you walk in, it's a strange way of living.

Panel Speaker - Male

I think it's a different way of living and they're doing it willingly. They go to Facebook and they put everything they do, they take pictures of the food they eat, they take pictures of the shoes they're wearing as they're walking down the street. They're putting everything on Facebook, they're already making it available. This kind of goes back to New York University had a discussion with a bunch of lawyers, how do we tackle the deep fake problem, right? If somebody creates a video and you can't tell that it's a fake and they can blackmail you with that video, what does the industry do about it? Do we watermark, do we go to every single video camera in the world and make it watermark pictures and video? Just completely unrealistic. The discussion went quickly down the path of well if every video is a fake, you stop trusting the videos and that's the world you live in. It just changes.

Panel Speaker - Male

Everything is fiction.

Panel Speaker - Male

That's not good.

Panel Speaker - Male

It's basically what he's saying. Everything is fiction, you approach everything as fictional.

Panel Speaker - Male

So how does - well that's how a whole other question, how we function. Let me switch gears here for a second. So we've heard about some new technologies like 5G and obviously the internet of things is now happening. What's going to happen? You can't change the password in some of these things. If there's a meter to your electrical - electric meter hooked up to your house that's connected to some smart grid, isn't that stuff hard coded? I'm getting some looks here.

Panel Speaker - Male

There are wicked problems, right?

Panel Speaker - Male

So what should we be doing with that?

Panel Speaker - Male

I think in general you're seeing a change in the industry to put security first into products. Before there was a rush to market to put things out there, to see if they succeeded. He's

trying to see a tide, a changing of the tide, because of all the security threats and vulnerabilities that are out there that the consumer is well aware of, that the companies are starting to build in security into these home products.

Panel Speaker - Male

How does a consumer, how does a company know which ones have that and which ones don't?

Panel Speaker - Male

That's problem 1, you can only test security and then never get [deployed.]. Somebody says they're secure…

Panel Speaker - Male

I don't think they can hear you.

Panel Speaker - Male

Sorry. You can only test security in a negative way, so that's problem number 1. Number 2 is I think the industry is still not really mature on security. If you see a credit card company promoting PCI DSS and not even complying themselves in a basic way, it's do as I say, don't do as I do.

Jan Guldentops

There's a flipside to this and that is as we migrate everything to the cloud, your IoT devices are most likely being controlled by some company that has a cloud presence. We had this conversation yesterday. One of the things that we can do to tackle this problem, because the skill shortage and security, the turnover, the fact that we can't keep up with living through it, we can't patch all of our servers. We can just go down the lists of all the things we can't do. As soon as you move all that to the cloud it becomes the responsibility of the cloud provider. Those guys are capable and they do have the staff and they do have the money to invest, to secure those things. So there is some advantage for at least that movement and if your IoT devices are not on a separate VLAN, that's completely shut off from the internet.

Panel Speaker - Male

I don't disagree with you, Jan, devices are always going to be hackable, there's always going to be human error in how people set up their networks and how they set up their home devices or work devices. But slowly we're raising the bar, the barrier to entry for organised crime is getting slightly higher than it was five or even three years ago and that is a success for the private sector, like Ted's company and law enforcement. As long as we can keep more people out of thinking about cyber criminals because it's just getting too hard, we're winning a little bit of the fight. Maybe not the whole fight, we're winning a battle maybe not the war, but the barriers to entry are important.

Vik Phatak, NSS Labs

So I think we have a bunch of audience questions. Any questions?

Panel Speaker - Male

One last point and it's basically I'm a bit more pessimistic. I've been doing these kinds of panels for 23 years now and I got out the presentation of 23 years ago, which made an overview of what we should fix. I used it in a new presentation and said what have we fixed already? We had theory for everything, but we're still using user IDs and passwords, we're still not sending signed emails, which if you would have told me that in 1996 that we wouldn't be doing that now, I would have thought you were mad, but we're still not doing it. We're still not going to the essentials and that's why I am pessimistic. We made progress, especially in law enforcement we're doing quite a lot of things, we're tracking money better which is basically the biggest clue. I think we're not there yet.

Panel Speaker - Male

It seems like I was [unclear] I don't see a lot of new things. I see a lot of products, but they tend to all be let's say recycling over and over again. I have to say, Ted, that what I saw today was pretty cool.

Ted Ross, SpyCloud

Awesome, thank you.

Panel Speaker - Male

It's cool stuff.

Manek Dubash, NetEvents

I think we've got a question over there.

Anthony Caruana, CSO Magazine

Thank you, Anthony Caruana, freelance from Australia. I think what Jan just said is really, really important to understand, but why can't we change? We all know that we're not changing, we know passwords are crap and we've lived with them forever. We know all this stuff is no good, everyone in this room knows it, I think everything journalist in here has written it about 50 million times. What is it that stops the world from actually moving on and what can we do to change that?

Panel Speaker - Male

Somebody from Cisco, John Stewart, actually gave a really good presentation recently. He looked back at the last 10 years and made the point that again everything has changed. Back in 1996, if somebody would have asked you if you'd be using the cloud you'd probably laugh at them. It's a buzzword. Now everybody's on the cloud.

Panel Speaker - Male

We wouldn't know what it was, right?

Panel Speaker - Male

So everything has changed, username passwords and part of the reason for that is there are so many new ways of digitalising your products. The proliferation of applications and all these different things that you need to log into, the easiest way to log in is with the username password. So they're not going to invent some new technology to release a new app. The apps are just everywhere at this point and they've taken advantage of the old authentication methodologies. But I do think we're on the verge of seeing some change. There's a number of vendors that are out there that are trying to stop - change this to make passwordless technology. In 10 years hopefully this problem will no longer exist.

Panel Speaker - Male

Ten years?

Panel Speaker - Male

Maybe 15.

Panel Speaker - Male

Yes well, we'll be retired by then.

Manek Dubash, NetEvents

Sorry, guys, we do need to end it there. We're out of time.

Vik Phatak, NSS Labs

Thank you.

Manek Dubash, NetEvents

Thanks Vik, thanks to the panel. Interesting stuff.