25-039B Fraud Event meeting - Ransomware - V2-L-Res

0:00
What is ransomware and what are the red flags that we should be looking for to prevent ransomware?

0:06
So so typically ransomware occurs when a an individual in your company has been has been phished in some way.

0:15
So they've received an e-mail or a text message that has a link or an attachment to that e-mail that contains what's called malware or malicious code.

0:28
And so once they, they click on that, that e-mail attachment or they visit that link that's in the embedded in the e-mail, it downloads code into the network that enables a wormhole for the fraudster to be able to penetrate into your network and determine, is there data in this network that I can, that I can monetize?

0:49
Or is there something that I can do in this network to, to hold this company for ransom to be able to gain access back to the network?

1:00
So what they do is basically freeze the network.

1:03
So the, you login, you go to login that day, you get the blue screen of death or, or skull and crossbones.

1:10
That's, that's the way they do it in the movies.

1:12
It doesn't really work that way, but it and and it basically says your system has been compromised.

1:19
You now have to pay us $100,000 or what would that be 3, two or 2 1/2 or three Bitcoin that you now will need to pay us in order to get the encryption key to be able to gain access back to your network.

1:35
So the thing to realize in this is it is you may pay the ransom key to get that encryption key, but they've got your data already.

1:44
And so typically what's happening while you are negotiating with them about how much ransom

you're going to pay to get access to your network, they're mining through your network to find data that they can monetize.

1:57
And So what they're going to do is they're going to take that data.

2:01
And depending on your the, the business segment of like if you're in the healthcare industry as an example, you're going to have patient information, you may have doctor information, you're probably going to have Social Security numbers, all this kind of data that they that a fraudster is going to be interested in.

2:18
And so they're going to take that data and advertise that data for sale on the dark web.

2:24
And So what happens is you've paid the ransom, you've gotten the encryption key back, but your data is gone and they've got your data already.

2:33
What they likely will do is come back to you again with another ransom demand because they, they say, well, we told you about this part of the data, but we had section had access to your network in another section of data that we didn't tell you about to begin with.

2:49
So now you've got to pay us again to get access to that that encryption key.

2:54
So most of this occurs almost always through through phishing, through infected software.

3:02
We even heard of cases where the fraudster would write something like year end bonuses on a jump drive, you know, the little plug in USB jump drives and it would and they'd leave it in the parking lot.

3:14
Well, some unsuspecting person picks up that that jump drive, looks at it goes, oh, you're in bonuses.

3:20
That's pretty.

3:21
That's with some pretty juicy information.

3:23
I wanted to take a look at that.

3:25

They plug it into their laptop or into their computer, and then it downloads that malicious code into their machine and allows the fraudster to have that access.

3:35
There's even something now called ransomware as a service.

3:38
And believe it or not, for about $500, a fraudster who is less technologically astute can go on the dark web and buy a kit that that provides them with the malware they need to perform ransomware.

3:54
It provides them with the instructions on how to do it, a list of about 10,000 e-mail addresses that they can use for their phishing e-mail.

4:02
And believe it or not, if they have difficulty with that, they, there's a 1800 number that they can call to get instructions on how to do it.

4:10
They'll provide them with customer support.

4:13
So again, it's a part of this virtual marketplace and it's, it's incredible how they are able to build this network and, and leverage these tools to be able to help perpetrate the fraud.

4:26
Yeah, definitely organized crap.

4:29
Exactly.

4:29
It's extortion.

4:30
That's exactly what it is.

4:31
And, and so it really, really it's so important that you have adequate backup plans just like reconcilement.

4:38
If you can reconcile daily, if you can back up on a real time basis, then you know that all you lost was just the last few minutes.

4:47

If you can back up on a daily basis, at least, you know, the only data that you're going to lose in this situation is it is the data from today.

4:56
So you want to make sure that you can then tell the the ransom or the person demanding the ransom.

5:02
We're not paying because we have an adequate backup and we know that we can restore our systems without having to pay the the ransom.

5:11
And you know it again, as I mentioned earlier, key, the fraudsters are completely indiscriminate.

5:16
They don't care if you think about a non profit nonprofits may say, as you mentioned, our business is not big enough.

5:23
We're not we don't have that much revenue.

5:25
We're not going to to be a victim.

5:28
That's just not true.

5:29
And because what you have and donut donor data, you've likely are using a credit card platform to accept donations.

5:39
The kind of things that you really don't really think about and the way that you're accepting those funds and the information that you're storing is all valuable to the fraudster.

5:50
I personally was attacked on a different level.

5:53
I had a fraudster reach out to me and say if I didn't give them so much in Bitcoin that they're going to release pictures of me.

6:01
You know, the only embarrassing part of the pictures was how boring they were going to be.

6:07
I personally rolled the dice and you know, I was not embarrassed by boring pictures of me getting in and out of my car at the bank.

6:16
But it's, and you know what?

6:18
I'm still, I mean, they're, they're trying everybody all the time.

6:22
And I'm surprised at the ransom amounts.

6:26
Some studies I read this past weekend indicated anywhere from 10,000 to $100,000, even in the consumer world.

6:34
So you know, the, the tech support scams that you see where the, they're posing as a Microsoft person that you've got a problem with your computer and then they ask for remote access to help you fix it.

6:47
Don't give them remote access.

6:49
That's that's immediate.

6:51
That should be an immediate red flag.

6:53
And when they're they're going to to get into your network and they're going to look for information in your computer that they can use.