The Scoop on Ransomware

CyberAware Podcast: Season 2, Episode 2

Nathan: All right, everybody. Welcome back to the cyberware podcast. This is episode two. My name's Nathan, and I'm your resident expert on all things cybersecurity. And I'm here joined with Ham.

Ham: Hey, how's it going, Nathan? It's good to be back on the mic. Once again, here in the broadcasting room as always.

Nathan: Welcome back.

So for today's episode, we're talking about all things ransomware, pretty hot topic in today's world. So I'm just going to start off with you. What do you know about ransomware?

Ham: Dude, I'm going to be really honest with you. I don't know a dang thing about it.

Nathan: Perfectly fine. So as I said, it was a big thing in today's world. Have you heard about ransomware?

Ham: Honestly it just from the stuff that we talked about, like in the last episode, that's really all I've heard about it.

Nathan: Okay. Well, I don't know if you're familiar, but there was a pretty big attack that happened not too long ago. So we're just gonna be talking about that today. And that's kind of the reason that this is going to be its own episode entirely. All right. So just starting off with ransomware, you know, what is it, how does it happen? And you said you are not,

Ham: I haven't the slightest clue.

Nathan: So ransomware combines, you know what ransom is. Okay. So ransom and software combines the two.

So as anything, ransom, you know, take something, hold it for money. And we have software, same idea. So what people will do was it's basically malicious software that go on your computer. And in most times it'll lock your computer out, lock your files and demand payment. Pay me in order to get these back.

So how this happened it could be anything as we were talking about vulnerabilities with people, someone might download something they shouldn't have. And, you know, with these big attacks, like I'm going to be talking about, it seemed, it was a bit more methodical and thought out with how it happened.

So, yeah, ransomware, a general gist of it is, it's malicious software gets on your computer locks out your files, and then, on the other end, those demands, Hey, pay me this much and I'll unlock your files for you. Or if you don't, they're staying locked, you're never getting them

back. So how it happens could be again with safe clicking, you could be downloaded something bad.

It could be, you know, someone's targeting you particularly. Or in particular. Yeah. Um, things like that and how, you know, ransomware itself, it might pop up sometimes, a common thing is they'll actually change your computer background and your, all your files get locked in. It'll just say in your background, Email or talk to this and, you know, pay this much.

Ham: That sounds so scary.Yeah. I can see that. See something like that happening on like, on a code grabbing website. I'm not going to say them, but like you go to this website and they'll give you like a steam code, for a game and you can download it. But like, who knows what if that code is like a legitimate thing.

Nathan: It always goes back to safe clicking. So when it comes to ransomware people themselves can be targets . You know, I don't want to forget that at all, small businesses, large businesses.

But it's surprisingly is that small businesses are actually somewhat bigger targets because they can't fight back, in most cases.

Ham: I can see that.

Nathan: So big businesses, like the one that we're gonna be talking about what they I'll just let everyone know REvil.

I don't know if you've heard of that group at all. All right. Well, I'll just let you in. They just hit for a $70 million ransomware. Oh, my word. Yeah. So, yeah, 70 million, so, it happened with JBS big beef, distributor.

Ham: Yep. Yep.

Nathan: It basically got associated with a bunch of their smaller clients or, what's the word I'm looking for partners, you know, smart people who rely on them and it happened with them and their information got locked.

So it turned into thousands of little or businesses. And maybe the mom and pop shops. Got their stuff affected from that. And then they ended up losing money depending on what's going on.

Ham: Oh man. That's so awful what in the world.

Nathan: Ransomware itself, , it's not a perfectly time thing, for some bigger instances, like Revil there's this big group.

They were probably methodical. They were thinking it out they targeted. They might've gotten it on the network and then, or a device and they might've waited and then finally, pulled the trigger. They went for it.

Ham: What I say a lot. When I'm gaming is a, the full send. I send it full, send it all the way, no holds going for it.

Nathan: And when it comes to these attack, sometimes it can be full send. Some times these things are just like automatic. Like they might have scripts in place where it's on the computer.

We'll do this, this, this other times. It's someone, it's a person who said. And going through the steps to attack, they're being step by step by step methodical in order to attack by themselves.

Ham: So Nathan, about how long does it take for like a ransomware attack to really like set in and get in place?

Nathan: That completely depends. You know, it could be something automatic. It could be a scripted thing, I guess, on a device that just executes or it could be something like a person or an attacker sitting there step by step , going through the attack, they're executing it the exact way they want to be

Ham: sure.

Nathan: And you know, this, some of this stuff, you know, it could be waiting for something to happen or it could be waiting for you to log in again, not everything's just, okay. It happened. It's on my device. It's going to instantly go through some of this stuff could be waiting, could be lurking, just waiting for special circumstances. And then it's going to go through.

Ham: Okay. Interesting. So like, you know, just, you know, we'll bring it back down to, instead of on the big company level, we'll go back to the mom and pop kind of shop kind of level. Someone could be in a coffee shop. Right. And they're chilling. They're like, and they're on the network, they're on the free network.

Right. And they could potentially be sitting there just gathering information, getting themselves they're warm in their way in there, something like that.?

Nathan: Yeah. Potentially.

Ham: Okay

Nathan: You know, ransomware, a lot of it is. When it comes down, you know, as I said, it's a lot of software at the end of the day, so you got to get it on their device.

And I'm sure there there's a ways to do that. Either having them download something, they shouldn't be, or again, if you have their information, like you were saying, you know, that's another way to do it. But a lot of the time you have to have either a device or be able to get on their device or their network in order to execute this.

All right. Uh, so yeah, just going off of real world examples, we were discovering R-evil. So yeah, the JBS attack, $70 million. And basically JBS was the big fish. And then all the little fish associated with JBS got affected, which is how that, that price came to be. So as I was talking about JBS I'm sure has a big IT group who was probably able to stop the bleeding a bit better than a mom and pop shops or the little littler shops who are associated with them.

So, what can people do? I mean, to prevent this businesses themselves as well you have a ransomware attack, what now? Just being aware of ransomware, you know, what's going on, what kind of attacks, if you have a group or, you know, who's doing this, or even if you have like a criminal, you want to know their M O who they go for, who they don't go for.

Things like that. It's good to be aware of that. Know if you're a potential target. No, why your potential target, where you're vulnerable and what they're going to be going for. Continuing on, real world examples, another big one. I don't know if you're familiar with wannacry.

Ham: I am not, no.

Nathan: Happened a while back, but yeah, basically, you know, attack a hospital. No, no one safe hospital, a hospital. What, what could they, like, what could they, what kind of information could they get at a hospital?

Ham: I believe they demanded money. You know, they're playing with people's lives, it's not like anyone.

Nathan: Oh, it's ransomware. It's just data. No, one's gonna get hurt. No, that's, couldn't be further from the truth. You know, anyone's a potential victim, as I was saying earlier.

Ham: That could, yeah, that could be like money medical records. You know, what kind of like what other account information you can have on those medical records?

Like your prescriptions, all that other stuff, like what's gone on in your past, like that's crucial information.

Nathan: Yup. And you know I don't know if you've heard of it lately, but the pipeline attack that happened not too long ago.

Ham: Ah, I've been in the dark about these. ' cause I, I don't see them covered on the media.

Nathan: Some are, you know, like this R-evil one very, very big news recently.

Ham: I think I saw something about this on the news, like you were saying, and it's just jogging my memory. I think they like described the attack.

Now, this is going to sound cheesy now. Pardon my pun. It's like different layers of Swiss cheese, stacked and stacked, like in a line because Swiss cheese, the holes are random. So they got to weave their way through each of these layers of security to try and get to their main goal.

Nathan: Yeah. I mean, at the end of the day, it's not like, you know, we're just sitting out, you know, we're just sheep sitting.

Our companies don't have anything going on. Some companies might not be very well protected, but you know, something like JBS they have a full staff, things like that. Like very, very well thought out plans. As I was saying earlier, it's not a walk in the park in order to attack these guys. Most times they're protected.

They've got defenses. They're defended pretty pretty dang well. So, you know, Just that sort of thing, you know, it just goes to show you now when these groups want something, they can get it.

Ham: Oh, absolutely.

Nathan: I don't know I mean, even just going off cyberware attacks and just in general, I don't know if you know, solar winds, if you've heard of that.

Ham: Not a clue.

Nathan: But big, big government contractor for our military. And, they got backdoored this year.

Ham: What is backdooring?

Nathan: So basically, someone's just going to get their way into the system there as again, you got the front door, you got the back door. They're sneaking. Through a different path, as you were saying with the Swiss cheese, the different holes, they're bypassing everything, sneaking their way in, into the system, into network, whatever it is.

Ham: That's huge. Especially for US military . Yeah.

Nathan: Okay. All right. So Nathan, let me, like, you've been naming off these like attackers who are these people, you know, a lot of times, no one really ever finds out. It could be anyone it's not, you know, it's not necessarily a bunch of people sitting in their basements, hacker voice I'm in.

It's not always like that. It could be a group of hackers. They might've met and they just wanted to do this together. They, it could be okay. There are a set group who does this all the

time. Again, it might just be some people who are like, familiar, Hey, let's do this, and it could be anyone from a group to a single person to anyone attacking.

It just depends. What their motive is, who they are, what they're doing.

Ham: Stuff like that , it seems almost an incredible level to reach, especially going for like a 70 million dollar deal.

Nathan: As I was saying earlier, not a walk in the park, these people are not stupid.

No, they're very, smart with how they do this. And you've got to think of the work that goes in order to do something like, oh, I'm sure it takes years of prep.

Nathan: Sometimes it does. Yeah. As I was saying, we were going off Solar Winds or. But, I mean that trumps all of their cyber attacks in history, hands down, and even with there are even when I think that's now the biggest ransomware attack that ever happened. Wow. Yup. They are getting a lot of money for this sort of thing. And I hate to say it, but I'm sure it pays pretty well. Don't recommend anyone doing this . And as we were covering earlier, you know from what I've heard, R-evil's gone dark.

Ham: I believe that.

Nathan: because they were being pretty open on the internet, things like that, you know, talking and reaching out to community, whatever it is and about what's going on with them. Sure. Yeah. So they just kind of went in the dark.

Ham: Now Nathan, what can these big companies do to stop these kinds of ransomware attacks or what can they do to recover.

Nathan: Yeah. You know, there's a lot of times its good to know, you know, identify your vulnerabilities, protect them, detect and recover.

So that's kind of the main as good like practice right there. Identify protect, detect, and recover, you know, as far as businesses, big, as you mentioned, small and even personal, you know, have something in place, you know. Ransomware, the main goal is to get money. Most times they're going to demand a certain payment.

Okay. This happens. Here's how we're going to proceed. I recommend having a plan of attack in case something like this ever happens.

If you have contingencies in place, you might have something like cyber insurance.

Did, you know, cyber insurance was a thing?

Ham: I never knew cyber insurance is actually a thing. Can I bundle it with my car? My ATV?

Nathan: No, there's no little green gecko for this, but no cyber insurance, basically businesses, Can get cyber insurance in case something like this goes down, or they might lose something like their data or what not.

They have this insurance in place to, you know, get it back or help them refund the loss, whatever it is.

Some companies, you might have policies in place, or even you might have contingency plans.

It's something that's a good talk to have with your company. So I know that we've talked about it with our security team.

We know what our plans are. And I'm sure a lot of other companies have it. It's good to have a plan in place, you know, and having, you know, in case sort of things happens. You need a plan in place, talk to your management, talk to your ITs, figure out what you guys should have in place for this. Cause it's better to be prepared that have this happen.

And you're just left out in the open, trying to scramble to figure anything out or everything out.

Ham: Imagine being in the dark when something like this goes around, you know, like it could be one day you're at the office, you're chilling, you're hanging out. And next thing you know, like the people on like the second floor and all their computers read the same file name, like log in here, do this, do that or whatever, or if not pay us, you know, $70 million. Like that would be so scary. Like imagine being there, imagine, you know, you wake up in the morning, right? You go, you have your morning coffee and you get, you know, you'd drive a 45 minute commute through traffic.

And next thing you know, you're at the office and holy Molly, my computer has the message on, everything's gone. What do we do?. Okay. Call IT of this, you know, of this branch can't really do much. Call the bigger guys. Yep. They can't do anything. Okay. Call the bigger, bigger guys.

Nathan: Yep. And speaking of you know, the bigger, bigger guys this ties into, you know, again, have the plans in place, but there's also things where like, if you have this happens by a group, it can get tied in with, you know, government like FBI might work the case with you because you know, it might be tied in or they'll come help or stuff like that. I mean, it's, it's a pretty big deal when it happens, you know, and going off the cyber insurance, as I was saying, your plans in place, you might have cyber insurance. You might not, your management might not want, right.

But if you guys do, you know, if this happens to you. First thing to do, talk with the management, talk with, you know, figure out what you get plans you have in place and act on them, you know, and go from there. You know, if it's okay, we're going to go talk to our cyber insurance people and go get this, go do it.

You know, you have those plans in place and follow them. Cause it's gonna, biggest thing is you gotta stop the bleeding and that's pretty much anything IT, or IT security stop the bleeding. stop the bleeding itself just means, you know, stop any more issues from arising. Anything bad happening. You try to stop it as fast as you can. Like can these big corporations are there, like besides, you know, just the insurance are, they're able to like back up their files, backup, um, the important informations that they have. Great, great, great topics.

So yeah. Um, a lot of people have things in place, backups, data backups. So, you know, maybe once a day they might back up everything, but then if something like this happens, you still lose a day, but it's better than losing everything. That's true. But I mean, this goes for small businesses, being personal. Backups great, great thing to have in place in case you lose it, you have your backup that you can fall onto and no, no harm, no foul minus a little bit depending.

But yes and when it comes to ransomware, backups are the golden egg when it comes to, if something were to happen.

And then just get your data back from your backup. And, but I mean, this can, this can be a double-edged sword sometimes because if you have your backup stored on your network with the rest of the stuff, or if they're able to get in, if it's on your network, they might be able to get.

And then, you know, block your backup as well. You know, then you're kind of out of luck. Yeah. Oh my gosh. Yeah. So you just got to, we're going to be covering backups actually in a later episode. So we're going to be covering data and backup. So, you know, just stay tuned for that, but yeah, backups themselves are a really, really, really great way.

They're always like the best that you can possibly have in place. And even not even just from ransomware attacks, attacks in general, having this fallback. Yeah. In case anything happens, you know, and, oh, we got a ransomware attack, but you know, oh, you might've lost, you know, three hours or a day of work, but it's better than losing everything weeks or a month's worth of like, since he last backed up and I mean, for anyone listening, this goes for people, businesses big or small or anything, you know, have your data backed up, you know, whether it's on a hard drive somewhere or it's on a different wherever it is, I get it and make sure it's safe.

Ham: So yeah, I knew a hundred percent.

Nathan: All right. So as I was saying, you know, backup's, super important, highly recommend them. They're great. I mean, whether it's you a big business, small businesses and your personal life, great idea to have, and, you know, backups themselves, you know, as I was saying earlier, backups can still get, you know, targeted, vulnerable and there's, and this falls back to just the cyber insurance, you know?

Okay. We don't have a contingency planner, this is happening. What can we do? There's actually a thing in place called a ransomware negotiator.

Ham: Okay. Now, does that follow like the same lines as like, you know, I know the police have like a hostage negotiator that they'll call and if there's like hostages in a bank or whatever, have you like, is it kind of the same thing?

Nathan: I mean, I compare them pretty similar together. So the ransomware negotiator, as you'd say with the hostage negotiator, if you imagine your data, your information's the hostage, they're going to be the ones communicating with the ransomware group or the attackers and, you know, talking about, okay, you know, here's what we're going to do.

How much do you want? They're going to negotiate. You know, it might be something like prices or whatever's going on, what you're going to get. What do you want? Yeah. So, I mean, I think it's a pretty cool thing. Cause I originally didn't know negotiators were even a thing. But yeah, there's actual people who it might be through cyber insurance or there might be someone who is connected to your company.

Or as I was saying with contingency plans, they might be your contingency. So these people will, you know, fight on your behalf and just negotiate on your behalf to you know, negotiate. I, but yeah, as I was saying, yeah, hostage negotiator, you are very on the dot with how similar those two are. Cool.

You know, that, that seems so interesting because like these guys, you know, they'll be a part of this contingency plan and they'll, they'll go out and these, and they'll talk to these people that are creating such a harmful attack for these businesses and try to stop whatever they can. And I mean, as I was saying, you know, negotiators, they can work on part of the insurance.

And as I was saying, FBI can get involved or government groups could be, there could be through, there could be through law firms, because again, with law firms, you have those tied in with, you know, the money side of things. Yeah. Your data. So, yeah, I mean, it sounds like a really cool job. I haven't heard of it before, but you know, it sounds like the thing and these negotiators, they might be, as I was saying, you know, different, groups have different mo's different targets, things like that.

These negotiators can actually be specialized. I know this group, or I've worked with this group before I know their mo. I know what they're doing. Who they attack. I know how they, okay. What game they play? You know, I know, I know their plates, so it's kind of cool. Cause these people are especially, can be specially trained to sometimes just generalize attacks versus.

I've worked with this group. I know like they're specialized okay. With them. Like they know their playbook and they know they're going to do it. It's a pretty cool, it's pretty cool to learn about. So, yeah, I mean, you know, ransomware big topic nowadays, I would highly recommend, you know, if you aren't familiar with it and anyone who's listening, get, you know, go do some research on it, you know, maybe become a bit more aware.

And with the, any of the attacks we listed, like R-evil, pipeline, WannaCry. Those are great things read up on it and you can truly get a scale for just how devastating these kinds of attacks can be. So again, Ham, thank you for joining me on the second episode here.

Ham: Thanks for having me yet again, as being, you know, just your average Joe kind of guy like knowing and learning more about these things every day is a completely new experience.

Nathan: I'm telling you, it's fun to see someone learn all this stuff. You know, I like hearing people taking interest in this kind of stuff that I have.

Ham: I guess, Nathan, my top three takeaways from today's episode I say is like the scale, the amount of that these guys can bring to the table and how they're just able to just get in there and destroy something that's been building for years and years and years. I wasn't even aware of like these.

I wasn't even aware of cyber insurance. I think that's so cool. You know, they have the, they have their ways and they got their plans to deal with these cyber attacks and deal with this ransomware.

Nathan: It's not even just ransomware. I think about that. It's cyber attacks, cyber insurance for all these different texts.

You have phishing, ransomware hacking, you know, all of these. You know, uh, potential things that can happen. This cyber insurance could cover that. Cause I mean, it's not just ransomware where you can experience loss. Yeah. It's all these sort of things. And in this case, as we were saying with things like wanna cry, it's not just always about money.

It's not just money on the line or data on the line. You know, people can lose their lives and have lost their lives because of things like this. Anyone who wasn't aware of this, this goes back to being, cyber aware. If you can read up on these sort of things, be aware of what's out there and what potential threats there are in the cyber world.

It's always good to be aware of. And for you I'd recommend the same. Yeah, no, be, be safe. Y'all that's really all I got to say. Be safe, everybody. So yeah. Again, if you want more information on what it means to be, cyberware just go visit mnsu.edu/cyberaware. And again, thank you for joining us on our second episode here, and we'll see you next week.

Ham: Thank you so much.

Mercy: Hey everyone. Mercy Ayesiza here with the news. I'm a student expert on information security team. I'll be updating you with what's going on in this cyber security world. Before I get into the headlines, please make sure to subscribe to our podcast and today's highlights are ransomware attack on crystal valley, local fund Corp.

On September 19th, 2021. Crystal valley in Minnesota Best farm supply and grain marketing cooperative experienced at ransomware attack. The company based in the city of Mankato was able to confirm this through a Facebook post saying crystal valley has been targeted in a ransomware attack that tech has infected our computer systems and interrupted the daily operations of our company.

The attack on crystal valley came after another attempt by ransomware, a gang called black matter targeting an Iowa farmers collective called new cooperative. This attack was associated to have seized their computer systems, they asked for $5.9 million in ransom. Our second news update today. Army members and veterans combat transnational cyber crime syndicate a former us army contract and them for brick.

Frederick brown was recently sent us for stealing personally identifiable information from thousands of military personnel during 2014 and 2015 stolen information included names, social security numbers, military ID numbers that survive on contact information from victim. Brown send the information to a cyber gang who then use the information to access the department of defense benefits site and still millions of dollars.

According to the court document, brown was sentenced to 151 months in prison and order to pay $2.3 million in restitution on October 3rd, 2021, after confessing his role in this. Our third news update today 150 million Google accounts said to be automatically enrolled in two factor authentication. Google announced on Tuesday, October the fifth 2021.

It's intent to protect its users from data breaches by auto enrolling in 150 million user accounts and 2 million YouTube creators in two-step verification, commonly known as two factor authentication by the end of 2021. Googles Abdelkarim Medini, the group product manager working on Chrome mentioned that passwords aren’t good enough on their own. Gumi Kim director at the account security and safety team

added many times password 12 victim to being shared, guessed or stolen. Madini And Kim also mentioned that they are working to provide suitable technology options to help secure that content for the users who are non tech, savvy, and unable to enroll in two factor authentication methods. And that wraps up the news for this week.

Thanks for listening to the CyberAware Podcast. We'll see you next time.