Heather:

Welcome to the Hurricane Labs podcast. I'm Heather, and today we're going to talk about social engineering, including a few of the more interesting stories our team has to share. According to the 2021 data breach investigations report from Verizon, which you can find linked in our resources, phishing attacks related to breaches as a whole have seen an increase of 11% with social engineering attacks accounting for 69% of all public administration breaches that Verizon analyzed in 2021. To help with our discussion, I have Tom Kopchak, Meredith Kasper, and Dennis Goodlett. Thanks for joining me today, guys. I know you guys are super busy right now.

Dennis:

Thanks for having us.

Heather:

So before we dive into your stories on social engineering, let's talk a little bit about what social engineering is and why businesses should be thinking about it.

Dennis:

Social engineering is a very soft subject. Essentially it's how marketing works. It's how sales guys work. It's how conmen work. It's how magicians work. And it's just a means of speaking and handling yourself to maximize the potential that your target will do some behavior that you find desirable, which they may not have otherwise done beforehand. We're not going to completely get rid of this anytime soon. That's part of the reason why having good access controls and log management and being able to shut down stolen credentials quickly, those kinds of things is so important. I'm not saying that social engineering's impossible to stop, but social engineers that do this for a living have been caught by social engineering scams before. If someone finds a really good premise then it's hard not to fall for it sometimes.

Tom:

It seems like a lot of times there's a tendency to stigmatize people who fall for social engineering, but that's the wrong approach. Because it's, first thing, so easy for someone to get tricked by something like that, especially if the attacker is sophisticated. And if you stigmatize someone or punish them for that, it creates a situation where there's not incentive to report it. And we don't learn what techniques are being used.

Dennis:

Yeah, I 100% agree. I nearly fell for social engineering once because it hit on one of my blind spots in essence. I really don't know how some things work, like paperwork and taxes and those kinds of things, like organization I'm bad at. So if a social engineer says, "Hey, you're late sending this paperwork here," then I'm going to... My stomach will drop, I'll be terrified and think like, oh no, I'm going to go to jail or something. And I'll start to take care of it right away. I will really want to click that link. For someone then to like publicly punish me for it because of this insecurity I have in essence, I'm going to be really upset about it. I'm going to be... I'm not going to like the person that does that. We all have these vulnerabilities like that, that's why conmen still exist. That's why all the exit scams and stuff like that, because those desires that you have that if someone plays upon them properly in just the right way can get you to do something that you might think... That you might even know is a bad idea. Anytime there's

something that is difficult to understand or is a little bit confusing potentially, for me it's paperwork, someone can prey upon that to get you to do something you shouldn't. So I used to be a professional magician. So I used to do this stuff for card tricks all the time.

Tom:

I do got to say, I used to be a professional magician is the best out of context Dennis quote we could take from this whole thing.

Dennis:

That'll come up later in one of my stories actually.

Tom:

Awesome.

Dennis:

So one of the most popular books for social engineering I read when I was in high school studying to be a magician. Being a magician I hate social engineers in general, and I've mostly stayed out of doing social engineering. I've helped with... So I'm one of the pentesters. We've done social engineering engagements where we out mass emails and stuff, and we've also done physical pin tests and stuff in the past. And I've participated to some degree, but I always just feel terrible about it. Because it's essentially like I trained for a long time to be able to fool everyone, and now you're telling me that this fooling people is actually really malicious. That I can use it for really mean stuff rather than increasing the moment of amazement for a dumb card trick. So I try to stay away from social engineering as much as I can. I wish I didn't know this stuff because it can make you paranoid also. So I'll tell you my first story. My first day of work at Hurricane Labs, our office manager asked me to come sign some paperwork, but I was installing my system at the time. But the office manager wants me, I'm not going to keep her waiting. When I get back, I found one of our sysadmins was at my computer installing a back door. At Hurricane Labs you don't leave your computer unlocked. I was still installing so it was impossible to lock my computer, and that was the first time I found out you could go into a TTY from the installation screen. But we used to mess with each other like that, where we would add back doors or send out emails or whatever, if you left your computer unlocked.

Tom:

That might also have been the first time that I learned that you could do that from an installation screen too because it was pretty early in my career at Hurricane too when that happened. I remember that experience too so you weren't the only person who learned something new that day, Dennis.

Dennis:

Sadly, I think that day flipped a switch in me in like never again, and I became the guy that's adding back doors a little bit too much. I have a Ducky, a USB head device. So it's essentially just a keyboard but there's no keys on it, you just add a file onto the USB device that will tell it what to type. And so it types really fast. So if you plug it in, it's decent for taking care of servers and stuff. If you know you have all command that you want to type in every time to the same server you can just plug into each server. In particular, it's used to type in a command to the keys to immediately open a command prompt, type in a back door, and then close the command prompt in half a second. The problem is at Hurricane Labs

everyone locks their computer judiciously. We're very serious about locking our screens because there's people who are or are constantly looking. Every time we walk through the cubicles you can see people checking to the left and to the right. Like, are they locked? Are they locked? Are they locked? Are they locked? This Ducky, while it would be useful in most places, isn't very useful in Hurricane Labs to break into people's computers, because if I plug it into a locked computer it's just a keyboard. It has to type in the password before it can type in the key control to open a command prompt. And I don't know the password. So I've gotten a few people with the ducky just by getting them to look away from their computer long enough for the Ducky to be plugged in and executed. One of the times I did it was I snuck in an extra USB extension cord and ran it to the next cubicle so I could plug the ducky in from over there while someone talked to him. So someone came over and just said, "Hey, how you doing? I heard you got the new video game." I think it was Grand Theft Auto had just come out and he was talking about it, which definitely will get this guy to turn around. And he just has to not look at his computer screen for a minute for me to plug it in. So we rooted him that way. But the more fun one was someone mentions to the new person that I used to be a professional magician, and so the new person is like, "Oh, really? You'll have to show me a trick sometime," which is a normal expected response. This new person we've been wanting to break into, and so at that moment I said, "Yeah, I can show you something." And reaching into my pocket where my Ducky was. And then I did the oh face, like, oh what's... Oh, I'm sorry, Patrick. I still got your USB drive. And I threw my Ducky at Patrick and he caught it with a weird expression on his face that like, I didn't give you a USB drive. And this isn't a USB drive, I know this is your Ducky. Like I know this is the tricky thing. But then I said, "I'll show you a card trick." And proceeded to begin my show. And as I'm just getting started, I see that the whole room is watching me. I make it known that I know that the whole room is watching me, and so it would be better for everyone if I move over here so that everyone can see me. Over here was in the exact opposite direction of this person and their computer, so this person had to turn around 180 degrees away from their computer to watch the show. It was at this point Patrick realized, Patrick and Corey realized like, oh, they're looking exactly away from their computer and they did not lock it before they swiveled their chair around. So in the midst of my show, Patrick plugs in the USB dongle into this person's computer while their computer is less than a foot away from them, they're just facing the wrong direction. The payload executes and it ends up getting firewalled and I didn't get root, but otherwise it would've been a good story.

Meredith:

I think it's still a great story.

Dennis:

Yeah, I was really mad about that one.

Tom:

Once again, it's always a firewall problem.

Dennis:

Yeah, it's always a firewall problem. So the other cool story I have. Pentest was hired to do a mass email campaign to a company. We sent out a bunch of emails and we got a good response. From that we were able to steal passwords I believe. Within 10 minutes of sending the emails out, we got reported pretty quickly. And within 10 minutes we had a phone call from the sysadmin. That's like, "Was that you?" Yeah, that was us. All those emails you got, we did that. You caught us pretty quickly. Good job. We'll tell you who we caught and verify whether you found all the people that we caught. The next day rolls

around and we're still doing social engineering I think, but I think we have limited targets. And that day we're just brainstorming what we can do with those targets, when we get a phone call from the client who again was like, "That was you, right?" No, no, that wasn't us. That was... Someone emailed you? That's legitimate. That was a real campaign, that was a real hacker. So some poor hacker sent out a real email campaign the day after we did our campaign, so I doubt his response was good. And I'm sure of that because one of the people that we emailed, one of our targets, when they responded to our email we were spoofing the sysadmin, essentially. For some reason their email client decided that we were the real sysadmin and their sysadmin was not. So she was trying to respond to the sysadmin to say, I didn't fall for the second attempt at social engineering. But she responded to us. Which is a great story in that, one, I know that social engineering testing works to some degree at least, at least when fewer person fell for this. But two, also she fell for our social engineering a second time, so it's just a constant battle.

Tom:

And I think from a defense perspective it's easy to blame the user, but this attack can be anywhere from really simple to really sophisticated. And a really sophisticated one that's targeted is going to be something that people are going to fall for because they think it's legit and it's really well-crafted.

Dennis:

That, and so I've received emails at Hurricane that I thought is this phishing? But it was legitimate. Usually those emails are followed by one of our sysadmins or someone sending another email saying I set something up and so you should be receiving an email about this, which is great. But that confusion, they're like, if you have an employee that just randomly gets emails that are legitimate about stuff that they should be doing from outside sources that they wouldn't expect, then stopping social engineering is going to be near impossible. Because picking which one is legitimate and not is very difficult. So like those... Any process that has that type of confusion as to the identity or purpose that users regularly have to engage in, that they would get in trouble if they didn't engage in, is perfect for social engineering.

Tom:

Yeah, I think our user base is generally overly paranoid, but even with that there's clients that we interact with and new customers that have different processes. And we have to have that culture of communicating what people expect, because even if you try to send something legitimate, a lot of people will think immediately it's an attempt to social engineer them into something. Which is good, but even then not everyone's going to take the same level of caution as the most paranoid person, for example. So it's a risk any organization needs to at least consider.

Heather:

Meredith, I think you had a story or two that you wanted to share too.

Meredith:

I do, they're more shenanigan-based because I often get tasked with shenanigans versus crazy levels of social engineering.

Dennis:

Shenanigans are fun though.

Meredith:

This is true. I went to school where we got to learn a lot about acting, and I wouldn't say in an official sense manipulating people to get what you want, but hypothetically manipulating people to get what you want. One of the cool things about our industry is, for those of us who are security-minded and paranoid and not so trusting of the latest technology, every time that latest technology comes out we want to play with it to see how we can break it. Which is awesome, because I was able to get my hands on Google Glass at one point and Google glass has some fun little recording features and tools that you can use to basically use that camera that's on the front to either take a photo or record. And I brought those into my workplace at the time where I had already been tasked by the CISO to see if I could get any other credentials, and I started the recording and then handed them off to another coworker who happened to have domain admin and firewall admin. And said, "Hey, take a look at these. Look what I got my hands on." And then as they were looking at this, I went, "Hey, you forgot to lock your screen." So I went over and locked it for them. And then they sat down while having Google Glass on, and I got to see them stare at their keyboard and type their password. And it took quite a few times of reviewing that video, but I did get to get a password from a video recording.

Dennis:

Yeah, that's an awesome story. You just handed them the surveillance device to surveil themselves, that's a really good one.

Meredith:

Yeah, that's one of the nice little dirty tricks about Google Glass. And I consider that one playing a bit dirty, because if you don't know all of the features you wouldn't think that you could force it to just constantly record video. But you can make it work.

Dennis:

The office used to have a device that would man in the middle a keyboard. So you'd plug a keyboard into one side of it and then plug the other side into the computer and it would record all keystrokes. And so it was very important that you kept your office space neat, just to make sure that you didn't... It would be obvious if that someone plugged that in at some point. But I remember Tom would never type in his password to his keyboard, he would always type it directly into his laptop, at least for drive encryption password. And I remember him also closing his laptop over his hands so that no one could see even his fingers move. And then one day at a coffee shop, as I'm getting ready to type in my password, I realize there's a camera right above me. And so I've taken to doing the same thing, Tom.

Tom:

I think part of that was a side effect of that version of Linux didn't like using an external keyboard for the drive encryption password, so that probably was a forced on me sort of thing. But good side effect.

Dennis:

Yeah, yeah.

Tom:

And the amount of things that you can do with any decent security camera to be able to see details is amazing. Apparently except at banks that get robbed, they can't tell if it's even a person that robbed it because it's some really low resolution video. But like-

Heather:

It's Bigfoot.

Tom:

Yeah, basically. But-

Dennis:

Yeah, everyone has a full HD camera in their pocket but banks don't on their vault door.

Tom:

Yeah, but if you look at a modern high-definition camera that can zoom in on stuff, you can read the newspaper that someone's reading when they're standing down the hall, basically.

Dennis:

So Google Glass is a good illustration of... If you don't fully understand the technology that's around you, then little things like try these glasses on can drop your password. There's a neat attack that was presented a while ago, where if a microphone is near your computer as it's doing DPG operations or PGP. So if you're doing RSA encryption near a microphone, the microphone can listen to how hard your CPU is working and recover your private key.

Tom:

That just blows my mind.

Meredith:

It's terrible and I love it.

Dennis:

Yeah, it's some neat math involved, but you can pretty much see the modulars operation being done on multiplication... On the exponential stuff. The researcher was able to recover a private key using a cell phone microphone that was within a yard of the target computer. So a colleague coming over, setting his phone down next to your computer casually because he just texted somebody, and then asking, "Hey, can you email that guy those details?" He makes sure to sign the email also so he knows it's from you. You just lost your private key. So it's those in particular that like a premise that is reasonable, so it would be reasonable if Tom came over to me and asked me to encrypt an email to someone. It's reasonable for him to have a cell phone with a microphone and it's reasonable for him to set it down on my desk, I don't really care. But those things added up means I can lose my private key.

Tom:

Also, I think about the number of times where someone like Meredith will walk up to me and be like, "Hey Tom, can I see your phone?" Like, "No."

Dennis:

A restaurant I really like, their menu is only in QR code, which is awesome because that means I'm not touching stuff, which is great for COVID and all that. It is a little bit worrisome that I just take the QR code that they made, throw it in a garbage, and put my own here.

Heather:

That ties into your second story, I think Meredith.

Meredith:

Yes, and this also brings up a short, stupid thing that I did in college, out of curiosity, with QR codes, of course. Because people do scan the random QR codes and I ended up printing one out and ironing it on to a hair bow with on the other side just a fun little icon of this TV show I enjoyed at the time. And people were like, "Oh, what's that QR code on your bow?" I'm like, "Oh, it's a clip from my favorite show." In reality it wasn't anything malicious, it just led them to the original Rick Roll video. I was trying to teach people to stop scanning those stupid codes. So I had an interesting task given to me by that same previous CISO to attempt to get some active directory credentials for an organization. And I consider this a bit of a task failed successfully, if you will. I had some previous knowledge of the inner workings of the organization and what various systems and services they used. And I had a what I believed at the time was an insane premise, but I was asked to dial it up to 11, make it as obvious as possible that you were attempting to get credentials. And basically said there was this breach that happened with Facebook. I spelled the name Facebook wrong. Our company, our payment system was hit by the same breach so we are asking you to please click here to log in, update your credentials, and see if you have been affected by the breach. If you have been affected, here's how to turn on two factor. Here's what two factor is, and it basically... It was a terrible description of two factor, where it was you need to go buy an external card from a store. I ramped it up to 11 with crazy. And sent it out very broadly to all of the employees at this location, this was an educational place so there were both faculty and staff going to the same payment portal. And I was hoping to get active directory credentials, even though this payment portal was supposedly had separate credentials. But with the premise of I'm sending this out at 4:00 AM, people are going to check their email at six or 7:00 AM when they're not fully awake and put in their domain credentials. I ended up getting people who did in fact put their domain credentials in the first time and then went back and went, "Hey, Nope, that's not correct. That's not how I log in here," because it didn't take me to the login page. And then put the correct credentials in for that third-party payment processing system. And so I not only ended up with one set of credentials for many people but two, and the success rate on most of the domain credentials I got was around 80% when I went back to check a week later and generate their report. And for those that had submitted their payment processing company credentials as well, we notified them immediately, "Hey, you need to go change these, this was a phish." But those same people didn't go back and change their domain credentials when it was all done.

Tom:

And I wonder if part of that could be users maybe not realizing the differences between the credentials or the fact that maybe one credential was stolen, but not connecting that their domain credentials were also stolen. Just with the number of accounts that anyone has to manage I can see that be really easy to happen. And like to some extent, even using a password manager with the way companies change domains around a lot of times, you can't even necessarily guarantee that'll protect you.

Meredith:

Right, and I was fully expecting for people to go back in, take a look, and say, "Hey, I clicked on this link before, so maybe I'll go directly to the website." But people were going back time and time again and trying to update their credentials through the compromised landing page that I had built. That was interesting to me, because if at this point you've been told that this was a phishing email and the link in here isn't correct, don't engage with this fake website further, stop going back there to change the credentials.

Tom:

And that's almost a case where you need to find a technical control to keep people from going to that. But if you're in an environment where you don't have that level of control over your users, especially if they're doing this from home or on personal devices, how do you stop that? You don't.

Meredith:

And I'd have to go back and look at the data to see exactly how many people ended up clicking from home, but I remember that we got a response back to our phishing email saying, Hey, I can't get access to this site. When we realized, oh no, we were only hosting it internally and had to go fix that.

Tom:

Yeah, like I would think that if you controlled access to... Not controlled access to the site, you assume it's a third-party malicious actor that's hosting the site so you can't shut it down. But like proxy settings for your user base, you could basically say anything that's going to this URL, send it to a internal page that says, this is a phishing link, don't click on that. To at least stop that attack from happening and minimize-

Dennis:

Yeah, if you can push VPN configs and you expect all your employees to be always on VPN, then you could update the config I think to redirect. You can do that, right, Tom, you know that stuff better than I do.

Tom:

Yeah, it depends. Like if you're routing all traffic, you could just not route that IP address to the internet. Assume now if it's a shared host like everything is then there might be another chunk of the internet that they can't get to. But I guess if it's an attack against your organization, you have to deal with the risk and ramifications of that. Proxy is going to give you more control at the URL level, so you could actually stop that. Alternatively, if you control DNS for your users, you can basically just make that not resolve or resolve to something internally. So there's different things you could do to try to stop users from getting to something, but it relies on how much control do you have over the endpoint?

Dennis:

Yeah, I know at HL we can just black hole or kill IPs going externally from HL. But doing that from the people that work from home is a new challenge.

Heather:

Earlier you talked about social engineering testing in one of your stories, and we've talked about how here at Hurricane Labs we make it like a bit of a game internally to keep each other on our toes. But how can other companies test their vulnerability. Are do pentest normally include social engineering in the scope of work?

Dennis:

Hurricane Labs has dabbled in social engineering for a long time. Before I started, I guess we used to do more physical pentests where we would try to physically walk into a place. But to some degree it's very scary, because one of our testers had a gun pointed at them doing that. So-

Heather:

That's terrifying.

Dennis:

Yeah, so you can get... Potentially depending on where you're trying to get into, even if you're trying to get into some small mom and pop shop, if there's a off-duty police officer or someone a little bit too zealous or something, you don't know what can go wrong. So it's terrifying in that regard, but there are essentially ways of testing that where you're essentially trying to elicit information or elicit a certain response, like going to a website. And those tests vary from we've stolen domain credentials using social engineering, and then other times the client did not want us to do anything scary like that or like that in-depth. And so we just proved that a user clicked a link.

Heather:

How can an organization work to reduce their vulnerability to social engineering? What sort of things can they do?

Tom:

Disable email.

Heather:

Talk to no one ever, don't trust Meredith.

Tom:

That's true.

Meredith:

We always say that.

Tom:

I'm not sure, at least the first suggestion there of disabling email is going to be all that practical. I could be wrong, but-

Dennis:

You would cut down social engineering a lot, but also productivity.

Tom:

It's fine.

Dennis:

First I would worry about being able to shut down something, and that helps you, whether it's social engineering or ransomware or anything else that you want enough control of your network to be able to detect when something bad is happening early enough that you can prevent greater loss. And you want to be able to shut down whatever is happening early enough to prevent greater loss. And that helps essentially across the board, whether it's social engineering or other things, and all of those things are very deterministic, very hard things. Can you change someone's credentials? Can you lock this out? If these credentials are compromised, can you still get into your own system? All of those things that are yes or no answers, whereas like what emails could be sent to our sysadmin that our sysadmin would actually click a link is a much harder question to answer. So I would focus on the easy things that you know you can do for sure that are yes or no. And awareness is important just to make sure that users know what phishing looks like and that it exists, and that it's going to happen. And that they are equipped to deal with it. If all of your emails look like phishing emails even when they're not, then that's not good. And if responding to an email as if it is a phishing email when it's not, if that causes being reprimanded or ill effects or something, then that's not good either.

Tom:

I think technical controls are also good where you have to assume that the user is going to do the wrong thing despite their best intentions. And if your sole form of defense is your users can't click on bad links or be social engineered, there's more you got to do.

Heather:

All right. Well, thank you everyone for joining me. That's all we have for today. Check out our links for the resources that we've referenced in our talk and keep an eye out for our blog on social engineering, which you can expect next month. Until next time, stay safe.