Heather:

Welcome to the Hurricane Labs Podcast. I'm Heather. And today we're going to talk about malware by way of USB. Early last month, the FBI warned that a cyber crime operation has been mailing companies USB thumb drives laced with malware. So here to talk about this with me, I have Roxy our vulnerability management and compliance specialist. So thank you Roxy for joining me today. I appreciate it.

Roxy:

Thank you for having me. I love this topic.

Heather:

Well, let's dive in. Why is it a bad plan, Roxy, to insert a randomly received thumb drive? Like how do USB scams like this even work?

Roxy:

Well, a lot of people think that they would not fall for this scam because they would never put a USB into any of their devices. But what this particular group is doing is they are making it appear like it's coming from Amazon or Best Buy or another retail store, or it looks like it's COVID 19 related, COVID 19 information. And so it is very possible that anybody could fall for this and receive the USB and put it into their laptop. So right now what they're doing is they're targeting specific industries, but this could evolve into targeting C-level people directly. It could also evolve into targeting larger organizations or schools or places where you have a lot of people that might be interested in free materials, like free educational materials or things like that. This could evolve into affecting other areas as well.

Heather:

So when someone plugs in a USB device and it is laced with malware, what does it do exactly? How does that whole process work?

Roxy:

Usually this is something that's going to happen quickly and quietly. So you're not going to see it happening in the background. And what a lot of these USB devices are doing is they're registering as a keyboard so they can create input that results in the device installing malware. It could have malware already on the USB and the computer recognizes it as you interacting through the keyboard and it goes through the entire process without you even inputting anything into your actual keyboard, especially if you have your computer on auto run, where it automatically runs anything on a USB.

Heather:

So what if someone gets a USB drive in the mail and it looks important? How can people verify this thumb drive's validity, that what they've received is actually something legitimate?

Roxy:

I would always check with the organization or the company that it comes from. So if you look at any of the materials that come with the USB and it has a website, or it has something that you go to, don't go to that particular website or follow any directions that come with the USB, find out what the customer service number is for the company that it's claiming to come from and call their customer service and ask them if they're sending out USBs? Most likely they are not, this is not really an advertising campaign

that I've ever seen, but definitely check with customer service and if they cannot verify it for you, then don't trust the USB. Also, what you can do if you receive a USB at work is to contact your IT department before putting it into any sort of work device, because you could be one of many people that receive the USB. So they're going to want to investigate and potentially perform a forensic analysis. And, it could end up being not malicious at all, but it's better to be safe than sorry and to let them go ahead and do their investigation.

Heather:

Let's say someone comes to you and says, "Oh, no help, I definitely just inserted this thumb drive and I think it had malware on it. What do I do now?" What's the next step?

Roxy:

Contact your IT department as soon as possible, don't try to fix it. Don't just let it sit there and go, oh, I'll bring it up later. Definitely unplug it immediately, but contact your IT department as soon as possible because there could be some processes running in the background or something, and they would be able to save your files before anything drastic happens. But don't be too embarrassed to contact them. Don't be too embarrassed about plugging in a malicious USB. They should be able to help you and prevent further damage.

Heather:

What if you're at a small company and you don't actually have an IT department specifically? Is there anything, are we talking about, they need to contact someone like us that can do it for them? Is there any help?

Roxy:

Yeah. If they're at a small company and they don't have an IT department, that's probably something they should bring up with management as well. But contact management to see what the next steps are, because there are companies that can be hired or we would be able to help as well. We have people at Hurricane Labs that can do forensic analysis. So if you're one of our clients, that would be a great idea to contact us. Or if the IT department is overloaded or can't get to it, definitely contact to your managed service provider. And they can also refer you to someone, if it's not us, they can refer you to someone that would be able to help.

Heather:

It kind of sounds like the big thing here is that you take preventative steps to keep this from happening rather than trying to remedy it after the fact and hope for the best.

Roxy:

Yeah.

Heather:

So here at Hurricane Labs, we have policies that help keep us safe and compliant, which you help to write and review those policies. What are some key points that people should consider when drafting their own security policy when it comes to USB drives?

Roxy:

First of all, like you mentioned, preventative is the best measure against malicious USBs. So have a backup plan already in place. Write that into the policy. All critical infrastructure should have a backup plan. And if you can make sure that all employee laptops and phones have backups as well, because what you want to be able to do is completely wipe the devices if you need to, and then restore from backup, and you don't want your employees to hesitate to contact you because they're going to think, oh, no, I don't have backups. If I contact IT, they're going to wipe my device. So make sure you have those backups already in place, that backup procedure already in place and written into your policy. Also, you can write into policies that critical infrastructure not have unapproved USB devices inserted into them, or only certain people have the authority to do so. If you're able to place restrictions without affecting productivity, apply as many restrictions as possible on USB devices. And you can also include it in your bring your own device policy, a procedure for how you handle USB drives and things that come from outside of the organization. Also, write into your encryption policy how you're going to encrypt devices and encrypt all of your devices if you can. Also write about antivirus, that it must be installed on devices and make sure that the system administration team is equipped to be able to monitor and respond to any antivirus alerts. You can also have auto run disabled on devices. You can encourage the use of file sharing services so that people are not tempted to send files via USB to each other, pass USBs or mail USBs to each other. You can encourage the use of file sharing services, which are actually a lot quicker to use because you can do that over email and email can inspect any files that are attached to it as well. So if you have that set up, do encourage the use of file sharing by email if it's not something too sensitive, or there's no PII in it or anything like that, otherwise you can use a file sharing service. Also, you're going to want to describe in policy your security awareness plan and educate employees on not plugging in random USB devices, make it part of that security awareness plan.

Heather:

What's the bottom line when it comes to USBs and security, what's the big takeaway that people should get from this?

Roxy:

There's a huge misconception that it would be very easy to spot these USB scams. And that's not true. These criminal organizations are getting very creative and it's important to not only be alert and make sure to verify everything, but let's not shame people. If you're part of an IT department, don't shame people for falling for these scams. Because when I was looking into this and I was reading about the type of scam, I was thinking, you know what, I could actually fall for this, even though this is my job not to, and I know not to plug in USBs at work, I could very easily fall for this and plug one into my own personal device. So somebody that is even less security aware as me that might actually plug it into a work device, that's totally plausible that it could happen and it has no reflection on somebody's intelligence or somebody's knowledge. A lot of people could fall for this. And it's also up to organizations to properly train people and to properly give security awareness so that people don't fall for these scams. So the responsibility, it's not only on the individual, but on the organizations as well to provide that education.

Heather:

All right. Well, thank you very much, Roxy, for taking the time to talk to us about all this stuff. It's super informative and helpful. That's all our time for today. Thanks for listening. And, until next time, stay safe.