Managing Cybersecurity Threats in 2023 Ep. 1

PLUS Staff: [00:00:00] Welcome to this PLUS Podcast, Managing Cybersecurity Threats in 2023, Episode One. We would like to remind everyone that the information and opinions expressed by our speakers today are their own and do not necessarily represent the views of their employers or of, PLUS, the contents of these materials may not be relied upon as legal advice.

Before we begin, let's meet our speaker. I'd like to turn it over to David to get us started.

David Shannon: Thank you, Tyla. Hi, my name is David Shannon and I'm an attorney at the Philadelphia Office of Marshall Dennehey. I chair our Privacy and Data Security Practice Group. We handle all sorts of different data breaches, data security incidents, and other matters that are relevant to privacy and responding to data breaches.

Today we're here to talk about managing cybersecurity threats in 2023. I plan to provide updates on some of the issues that are currently increasing in 2023, or ones that we think are going to increase, or will be new to some of the insureds and insurers out there. This first episode is on cryptojacking.

Probably people have heard of cryptomining. A lot of people have heard of cryptojacking as well. But this is an increased risk for both businesses and carriers at this time. And we want people to have a better idea about what it means, what are the potential losses, and then, obviously, what are the claims and the damages that insurance carriers may have to face in the next year and beyond.

So, we'll talk a little bit about cryptomining, then get into cryptojacking, and then obviously at the end, talk about the coverages and the possible losses that you might see. When we first talk about cryptomining -- to give just an elementary kind of summary of what it is -- with digital currency or coins, you're going to have different types and there are hundreds, if not thousands, of different digital currencies out there right now.

Bitcoin, Monero, and some others are ones that people will hear and be familiar with. And the price fluctuates. For these bitcoins, and I looked it up today before we started, and I saw that Bitcoin is trading right now at about $23,000.

So, it's not a small sum when you talk about a large amount of Bitcoin or other cryptocurrencies.

But what we have with cryptocurrencies is, how do they get created, and the simple explanation is they get created with cryptomining. People are creating the blockchains, which are used to validate the currencies. And in that cryptomining, to validate them, you also then have new currencies or new coins that are created.

To understand it, a new blockchain can be created and you need individuals or, what's more likely now, groups of individuals, pools in some respects, that are solving these complex crypto mathematical equations or puzzles, they're sometimes called. And by solving these equations, that person or that group, that pool will then be rewarded.

They get to validate that blockchain, which then becomes part of that cryptocurrency blockchain, and they get new Bitcoin or new cryptocurrency if it's another type of currency. And these Bitcoins are, they're generated [00:03:00] about every 10 minutes. So, there is a lot of money that can be made if you can validate and then get the reward for the new blockchains and the new cryptocurrency.

So that's why you're going to see people that will then try and mine and determine what these equations are. The problem that's arisen is that the equations have gotten more and more complex. They're extremely difficult to solve, and that's why you've seen people that will join in the different pools to try and solve them so that they can get the reward or the new coins.

And to solve the equations then, you need a significant amount of computer power or computer systems. And we're talking about vast amounts of computer power because you want to be the first to solve these equations. And that gets very expensive. You're going to have computing power, basically, which is the electrical cost for running all of these servers and computers to figure out these equations.

You're also going to have cooling costs for all of these servers or computers that are [00:04:00] working nonstop to figure these equations out. So, because of that, it becomes very expensive to try and solve the equations and get the Bitcoin. And because of these costs, that's what has led to the cryptojacking, which is basically hijacking of computer systems to solve the equations.

So, these cryptominers may be doing it legitimately. And then, unfortunately, we have some other hackers or threat actors that are doing it illegitimately by hijacking the computer systems to be able to figure out these equations. And what they want to do is use the computer systems and use the electricity and the power of the systems to solve the equations and then get the Bitcoin.

So, they're going to use different types of cryptomining malware that lets the hackers infect computer systems, large systems, so that they can then turn around, solve the equations, and get the Bitcoin. And what you'll see is the hackers are looking for [00:05:00] large industrial companies, cloud services that are used by companies, large MSPs (Managed Service Providers), that just have a lot of computers, hardware, computer systems or cloud systems. So, they can use those to come up with the results for the equations so that they're able to get the Bitcoin. They'll hijack the computer systems to solve the equations and these costs then can be significant.

We had one case recently where it was a very large IT provider that used a significant amount of cloud service. The hijacking occurred late on a Friday night. So, it was not discovered until Monday and during that weekend period, 3,000 virtual machines had been created to constantly run the mining software and to run the software that's needed to solve these equations.

And what happens then, is that you're going to have hundreds of thousands of dollars for the cost of running those computers. If [00:06:00] it's a cloud service provider, like the example I discussed with over 3,000 virtual machines, that company had Microsoft as one of their providers. Well, they get a huge bill from Microsoft then for all of these costs that were incurred. And that's essentially cryptojacking. They're able to use your computers to solve the equations and not pay for the hardware, not pay for the electricity costs, not pay to keep the computers cooling. And it can occur without people noticing what's happening.

This is where you’re going to see damages. It could result in a slowdown of computers working, so you're going to have a loss of your work. You could have the computers crash if they're being so overused that it's not caught in time, and then you're going to have a failure of your system. All of this can lead to a loss of business interruption, potential third party claims, a number of issues that are going to arise for that company or for the company's customers if somehow their computers have also been hijacked.[00:07:00]

And as we talked about earlier, because of the expense of the Bitcoins or the other cryptocurrency, it can be very lucrative. There's a reason why the criminals are hijacking the computer systems to do this. They want to get the new coins. And the more that they can get over an extended period of time, the more beneficial it is for them to hijack your systems.

So, all of those things can lead then to claims. Those are what we're going to see, and people listening now want to know, what are the claims you're going to see? So, an insured has been hijacked, like the example I used with the company that had the weekend cryptojacking that led to all of the expenses.

They're then going to get a bill from their cloud service provider, or they might have their own bills if they're doing everything in-house, for a tremendous amount of electrical cost, and they may have costs for the hardware that's now been permanently disabled or could have been used in a way that makes it unable for them to continue to use it for the [00:08:00] system.

All of that can then lead to business losses or business interruption claims. And those can be not only for the company that was hijacked, but maybe for its customers as well, or its clients, and they're going to bring a claim that can come against them, that they're going to then turn to their insurance carrier for.

We also could see some incident response loss and claims. If a company has been hijacked for cryptomining, somebody has been in their system. You know that there's been some sort of malware or infiltration of the system. More than likely that company's going to have to have an incident response occur where they're going to have legal and forensic work to see whether anything else was done to their systems?

Did they lose any data? Was any personal information compromised in any way? All of those costs would be incurred too because of this cryptojacking. And you're going to need to see, does the policy cover that? An insured is going to say, does my policy cover those business losses? Does it cover the business interruption losses?

And then they're also going to [00:09:00] look and see, does my policy cover third party claims that are brought? Because not only was my system hijacked, but my clients' or my customers' systems that are connected to our system were hijacked as well. One of the ways that the threat actors really want to get as many computers to work on this as possible is to get a company that does have connections to other computer systems.

You get some sort of cloud service provider or some sort of internet consultant or internet MSP that will work not only on the computers that are in the company that's been infected, but also other computers that are connected to that company. Or, it's a large corporation that has hundreds, if not thousands or tens of thousands, of computers that all can be infected and all work right away to do the mining and quickly add up the cost.

So, all of those things are something that needs to be looked at and determined when you're looking at what kind of claims would potentially arise. And as for the [00:10:00] carrier and the underwriters, they need to look at what are we going to cover, what does the policy specifically cover?

When it comes to cyber insurance, it normally will have the basic cyber extortion coverage for a ransomware attack, it will have the IR response for a data breach or potential data breach. Does it also cover business loss/business interruption? And then, does it cover the hardware cost if something's been damaged and has to be replaced? Normally all those things should be covered in a good cyber policy.

But this is certainly a key thing to look at, whether you're the underwriter or whether you're the insured, to make sure that all of these issues can be covered if you have such a breach-- have such a cryptojacking occur. And at the end of the day, that's what it really comes down to. Cryptojacking is no different than any other cyber incident in which you're going to have potential losses, and then you're going to have real losses, and does the cyber insurance cover it?

And the claim will cover it and it can properly be [00:11:00] responded to.

PLUS Staff: Thank you, David, for sharing your insights with PLUS and thank you to our listeners for listening to this PLUS Podcast. If you have ideas for a Future PLUS Podcast, you can share those by completing the content idea form on the PLUS website.