Heather (00:12):

Welcome to the Hurricane Labs podcast. I'm Heather. And today we'll be talking all about the FireEye and SolarWinds breaches. Joining me today is tier three SOC analyst, Tony Robinson, Tony. Hi.

Tony (00:26):

Hey, how's it going?

Heather (00:26):

Good. How are you?

Tony (00:29):

Everything is on fire, but you know, I like it that way.

Heather (00:33):

I saw the news last night and I was like, well, tomorrow's going to be fantastic.

Tony (00:38):

Yeah, it was just like last night at about 10 o'clock. I better write something up now. This is going to be a show. And if I, if I need like 10 minutes to get coffee, I don't think it's going to be that great.

Heather (00:50):

Alright. So let's kind of kick it back to like what happened last week with FireEye? So last week the information security vendor FireEye announced that their suite of red team tools were among the assets and data that threat actors retrieved in a breach. My question for you, what is red team and what do they mean by their tools?

Tony (01:15):

So typically when you talk about a red team, like a, the term red team and penetration testers are kind of, sort of interchangeable there are a group of computer security experts that are normally tasks with breaking into a target network. You know, there's a, there's some sort of a contract or agreement between FireEye's red team and the company that purchases red team engagement. They say, we want you to achieve these goals, or we want you to reach this part of our network. We want you to try a boy touching these things and you have this amount of time, and here's what we want you to try and do. And typically, you know, they either reach those goals or they don't. And when everything's all done the red team or the penetration testers will produce some kind of a report that tells the customer here's the vulnerability as we found here's how we got in. Here's how we went from this initial access to, you know, reaching the target or reaching our goals. And then they kind of given them recommendations. Here's things that you can do to stop us from reaching this point in the future.

Heather (02:28):

So how did the threat actors gain access to FireEye?

Tony (02:32):

Well there's also a lot of rumor mill going out around that. So right around the same time that the FireEye breach was announced, there was also a vulnerability announced with some of VMware's virtualization software, some of their business management software. There hasn't been any kind of a conclusive link tie to it, but VMware released a vulnerability advisory at like a couple of days before FireEye went public with their breach. Then the NSA and the the NSA and DHS came forward and said, "Hey one of our customers or somebody that we know was compromised recently with this VMware vulnerability. And they did these things to, after they gained access to the network." And then like a day later, FireEye says, "Hey, we got breached, but they never said exactly how they got breached." It's possible that SolarWinds might've been involved, it's possible that the VMware vulnerability might've been involved, the timing is just, there's a lot of coincidences here, but nobody really wants to say how the initial access was gained.

Heather (03:47):

So with SolarWinds, what happened was the attackers through a third party, attacked an update that was rolling out and added malware. Is that right?

Tony (04:00):

Yeah. I mean for the most part a they, they somehow managed to get access to SolarWinds and like, depending on who you're asking around right now, like the rumor mill is running wild because I don't think SolarWinds or a Microsoft Office or FireEye wants to admit how it happened, but someone has pointed out that it was their GitHub account that got hacked. So what they did is they gained access to SolarWinds. They found the software update system. They put their malware into like legitimate software, like kind of make a piggyback or a backdoor off of it. And then they use that update that was pushed out to different customers to gain access to their networks.

Heather (04:46):

And so that update went out as early as March, but it wasn't, it was just now discovered.

Tony (04:51):

Yeah. So like there was updates that were out between March and June of this year, they were saying that if those updates that for that time period or were potentially affected. Wild stuff. Yeah.

Heather (05:06):

Crazy. Is it like, is there like a similar sort of, maybe not the same, but a similar sort of time lapse with FireEye where there was just discovered this past week, but it happened sometime before that or did they discover it fairly quickly?

Tony (05:22):

They haven't released a public timeline yet, but given that it's FireEye and I'd like to believe that, you know, the old saying the cobbler's children have no shoes doesn't really apply to them. It was probably pretty recent. They were pretty on top of things. I mean, if you want another example of a company that was on top of things, when a breach happened, the Sans breach happens happened a couple of months ago. The Sans cybersecurity organization, they they experienced a, a phishing attack and they had a couple of emails I've gotten compromised and forward that contained some customer details, but they discovered that really quickly. It was a matter of like three weeks before they had discovered it. And

then they contained it, let everybody know, Hey, this is what happened and here's our timeline. Okay. So I'd like to think that FireEye has kind of on top of things too.

Heather (06:16):

So with SolarWinds this is called like a supply chain attack. Could you explain that for us?

Tony (06:23):

So a supply chain attack is where you were where an attacker would attack a third party software company. Like let's say for example a good recent example or, well, historical example that happened somewhat recently was with the Ukrainian tax software company, MeDoc attackers managed to compromise the company and somehow got into their software build system and use that to push ransomware to a bunch of their customers. When you talk about supply chain attacks, it's normally an advanced attacker trying to compromise a software company that a bunch of different business verticals might utilize or take advantage of. You know, so if it's if you're targeting, I see organizations with industrial control systems like power companies, oil companies, things along those lines, you might try to target say Siemens, that would be a third party that a lot of those organizations that use those tools would have to go to they'd have to download applications and products from a Siemens website. So if you were to gain access to that third party and either make your traffic look like it's coming from Siemens or take one of their code signing certificates and use it to sign your malware or backdoor their software somehow, and get it into that actual target you want to get into that is what a supply chain attack would look like. And we've seen this in the past with Ukrainian software company, a MeDoc and their tax software going in compromise and being used to spread ransomware. We also see in this with the cloud hopper APT trying to gain access to managed service providers, or it providers for various companies and trying to leverage that access to get into other targeted companies that they may be interested in. So the idea is, is that you go after a third party that you may or may not be interested in, but your target is interested in that third party. And you use that access to your advantage.

Heather (08:40):

What's the risk level for individuals and what's the risk level for companies?

Tony (08:46):

So when it comes to SolarWinds they probably announced right on their website, that there are over 300,000 customers and they have them across all kinds of verticals in terms of I'm a third party supply chain. This is pretty significant for them to announce that they got compromised because just about every company that does any kind of it or server administration they use some kind of monitoring software and nine times out of 10 it's SolarWinds. So it's a significant threat to most businesses that this compromises happen, but in terms of individuals most SolarWind software is paying for software and its enterprise enterprise means having to pay for it a lot of money for it in most cases. So it's more of a risk to large organizations, enterprises, and businesses that it is the end of the day.

Heather (09:47):

What can companies do then to sort of mitigate this risk? And that may even to, to identify if they're at risk.

Tony (09:54):

One of the things that FireEye's been doing a lot of recently that I appreciate as a security researcher is that they release a collection of their indicators directly to a GitHub software repository. And that's what they did for their breach when their Red Team Tools got compromised. And that's what they just did recently for in regards to the the SolarWinds backdoor that they're calling SUNBURST. So they have a, a large collection of indicators there that contained that work indicators like IP addresses, domain and host names, and also a series of file hashes that can be used to say, here are the actual backdoor files or that are located. Here are the backdoor files that the actors use to backdoor different companies. They also released a couple of clam AV snort signatures and YARA pattern matching signatures as well. So I would say if patching the patching, the backdoor out, isn't an option, which SolarWinds has already released one patch for this. And they're planning on releasing another one tomorrow on the 15th, then your next best your next best bet will be to get some kind of detection in place to see if you are affected by this breach. When it comes to you know, this attack in particular with SolarWinds, the timing is kind of awful, you know, for a bunch of different reasons. You know, this is the lead up right up to Christmas and a lot of systems, administrators and security analyst, it teams SOCs. They're going to probably be as far away from a computer as they can right now, because you know, it's holiday it's vacation. And, you know, even in spite of COVID and us being told to stay away from one another, some of us just want to take a moment and chill and get away from the computer for a minute. So that's, that's one thing is that a lot of people take holiday leave and vacation time off right around this time. And then the other part is that a lot of verticals, especially the retail verticals, they implement change freezes. So even though there's a patch available for this SolarWinds, vulnerability due to change freezes, and I'm saying, no, you can't do any changes right now because this is what, the time of year that we made the most money don't touch. It don't do anything, you know, because of that, you might not be patching this until January of next year. So it's really important that if you can't patch this, that you have the mitigations in place to at least detect it and, you know, prevent access to that backdoor, you know, through the various network indicators or through the host based indicators that are out there.

Heather (12:52):

All right. Well, thank you very much for joining me. I appreciate it.

Tony (12:57):

No problem and thank you as well as basically in here.

Heather (13:00):

Sure thing, catch you later. In addition to this podcast, Tony has also written a pair of blogs regarding these breaches. So be sure to check out our links below to get the scoop. We'll catch you next time! For now, stay safe.