Heather (00:13):

Hi, welcome to the Hurricane Labs Podcast. I'm Heather, and today we're going to be following up on the breaches announced in December by FireEye and SolarWinds. Now, as you very likely remember, just days apart, last month, FireEye and SolarWinds, each publicly announced that they had been breached. Following their announcements, Hurricane Labs shared security advisories, as well as a podcast discussing the events. So if you want refreshers on those releases, you can access that content by following our provided links. Today, Senior SOC Analyst, Tony Robinson is back with us to bring an update on these breaches. Tony, thanks for joining me.

Tony (00:54):

Oh, no problem. Happy to be here.

Heather (00:56):

Well, let's go ahead and dive right in and start with FireEye. Have there been any developments since they initially announced the breach?

Tony (01:05):

Well, there haven't been too many developments. The only thing that I have heard of recently is that there was a, there's a site online where there are a group of hackers that are claiming that they have access among other things with regards to the SolarWinds for each that they have access to a couple of FireEye documents and access to their tools with documentation, for how to use them and things of that nature. This is a very recent development. It happened within the last couple of days. I believe solar leaks dot net is the site and nobody has anything that confirms whether or not what they have is actually valid. So aside from that the FireEye breach was more or less an open and shut case. They announced that they had gotten compromised and then released indicators to detect their tools because they couldn't be sure whether or not they had been fully comped or fully breached or whether or not they had been used by the attackers or not.

Heather (02:15):

Have there been any other damage as far as FireEye goes, other than the potential of their tools being misused?

Tony (02:25):

I mean, there's always the worry that they might have accessed customer records, but there's no evidence there hasn't been anything publicized that indicates any of their customers have been compromised or any of their data has been accessed. And I mean, if anybody is going to be eating their own dog food or, you know, doing the right thing and informing their customers and making sure that it's known that, you know, these things happen, it's probably going to be FireEye.

Heather (02:57):

Right. So with SolarWinds, I saw that in their filings with the securities and exchange commission, they were able to reverse engineer the code that was used and learn more about the tools that the hackers deployed. Could you explain a little bit about what they found?

Tony (03:20):

Well, one of the things that I had heard about recently I wanna say it was CrowdStrike that recently did an analysis of one of the tools that they deployed. So the thing that's really interesting about the breach is that, you know, of course it's a supply chain attack and we've been talking about, you know, how supply chains are kind of a necessary thing if you run a large enough organization. And it's kind of interesting in that they claim that they managed to gain access to their build system or their system that they use for compiling code and making different versions of their product through an open FTP server or with weak credentials. Then afterwards, it was claimed that the attackers, when they got access to a SolarWinds network, what they ended up doing is installing a piece of malware or code that when the SolarWinds Orion Software in particular was being compiled on this virtual machine or the system, while it was being compiled, it would insert the backdoor or the malicious code that they wanted to get shipped out to as many customers as possible. So it's not necessarily a case of the attacker has compromised a developer account and said, I'm going to dump this code here. And I'm going to put it up in a CVS or SVN or whatever they use for code management. It was, here's a piece of malware that I'm going to stick on the system that does the software compiling, and we're going to inject this code as the code is as the products being compiled or being updated. So it was really interesting to see how they did that, because, you know, a lot of people are saying, well, why wasn't code review being done? Why wasn't there a comparison being done? It would have been extremely hard to detect it. And I don't think that code review would have caught it.

Heather (05:25):

What does this mean for the security community then?

Tony (05:30):

I think it just means further introspection needs to be done in people's supply chains all together to be perfectly honest. You know, it's really hard to figure out what that looks like. Your supply chain needs to be trusted, and if it's not trusted, then you have significant problems. You know, some other organizations are suggesting to doing tabletop exercises where you say, well, one of my vendors got breached and it turns out it was a supply chain attack. And this particular piece of software that we use got backdoor, how would we recover from that? What will we do? Do we have any other vendors that we would be able to switch to while they are getting this supply chain breach, managed things along those lines, it's, it's a much easier said than done scenario. That's what makes it so hard to give proper guidance on, because it's just a massive problem. I mean, SolarWinds being a prime example here, I've been in information security for the better part of a decade all together. And even when I was in school and just getting involved in, you know, learning more about the it world in general, SolarWinds was a well-known name back then. So that just kind of gives you an idea of how long they been there and how much of a trusted name they are to have that supply chain and have that trust kind of breach is a pretty big deal.

Heather (06:57):

What sort of damage are we talking about?

Tony (07:02):

So there have been a couple of different organizations who say state that they have been impacted by the supply chain breach and that they might've been targeted by this adversary. Microsoft said that some of their code might've been viewed. I don't think that they said it was modified. They only had read, they have read only access to particular bits of code. F course, there was FireEye and their tools getting leaked. There was–I want to say Cisco said that they had similar issues. The Department of Homeland Security said that they were targeted. And the latest that I heard was he USAA Office of the Court, but that they claimed somebody tried to access sealed indictments in the pacer database and the law enforcement database where charges and indictments are stored where that's kind of public information with exception, of course, to sealed indictments. And I think that that was something that the attackers were targeting and,uthey are alleging that it was related to the SolarWinds breach.

Heather (08:15):

What's your general reaction to how all of this has progressed?

Tony (08:20):

I kind of want to take a minute and say like how fast the story developed and how quickly things kind of snowballed. I mean, at first there was, I had some inkling that there was an NSA announcement or a Cisco announcement stating that there was a vulnerability in this VMware product. And right after that statement was put out, FireEye said that they got breached. And then right after FireEye got breached on the 13th that Sunday night, you know, people were saying that SolarWinds had compromised and FireEye had put out a bunch of indicators and now I just logged in and got on social media and saw all of my colleagues from various other places talking about it. And I was like, this is going to be a big deal.

Heather (09:09):

Yeah. So I'm coming up on two years now with Hurricane Labs and I've got no prior technical experience. I was an English teacher for 10 years. So I'm just now starting to get my sea legs as it werewith all of this. And even I, on that Sunday, I was like, Oh boy, like I knew, like I'm going to be up bright and early. I'm going to have my coffee. I'm going to be ready to go. Because even I knew like this is going to be one heck of a day that we're going to be coming into.

Tony (09:37):

That same night. I was writing up advisories and blog posts and saying like, Hey, I've got this stuff written up for our customers because, you know, with the name like SolarWinds being around, as long as they have, they're going to have questions, they're going to want to know whether or not we got coverage. And then it turns out, you know, that SolarWinds said that up to a couple thousand of customers were affected by it. And that, you know, a couple thousand customers had installed the backdoored software, not that they had actually had been breached. And then another security company came into the mix and stated that they were attracting this group or this group of attackers since late 2019. So it's really interesting to see that over the period of about a month, how the story has evolved and how more details have come forward between now. And then it just kind of goes to show that, you know this was a pretty complicated attack. I know that sophisticated gets thrown a lot in thrown a lot in threat intelligence reports and reports by different vendors, but this was quite sophisticated because they had the patience to wait things out and ensure that they got access to the targets that they wanted With all of these people, you know, analyzing what happened and looking at the tools and trying to attract this group. Why is it that no one's saying absolutely people are saying, they're pretty sure it was Russians, but they're not certain it was Russians.

Heather (11:15):

Why is that an issue?

Tony (11:17):

Well, that's a whole can of worms when it comes to attribution of a threat or a threat group. People can say that there are hallmarks that suggest that this software was used by this group. It has something to do with being able to analyze the trade craft and analyze how the software is developed and how it might be similar to other pieces of software that have been observed in other attacks. And some security companies will say this software has all the, of a Russian campaign or this the way that they rushed in and they grabbed everything they could. And they didn't really care if they got caught or not. This kind of looks more like a Chinese campaign or they might just do code comparison and say, Hey, this code block, or this decompile part of the code is very, very similar to this breach that we saw in this campaign. So they can say that they are hallmarks or that there are there's a bit of trade craft that looks similar, but being able to say for sure, yeah, this is definitely the Russians, or this is definitely the Chinese or whatever nation state is targeting. The data is much more difficult. You don't really get that too much with threat intelligence and information security companies, because they don't have the sources and methods that say an intelligence community would have like one of the more interesting reports when it comes to advanced threats was FireEye and an apt one report way back in the day, you know, they had information that the Chinese were attempting to compromise multiple targets. They managed to get pictures of the attackers. They knew what building they were coming out of. And I mean, at that time, I want to say that there's no definitive source that says this, but to be able to get that level of data, you had to have been partnering with an intelligence community source of some sort, you know it might be national geospatial. It might've been the NSA. It might've been another source. I can't say for sure, but, you know, it's kind of hard to say to get that information or get that level of granularity to say it was definitely these guys in this country for this military or for this group, you know?

Heather (14:00):

Right. Alright. Well, thank you for taking the time to talk to us about all this stuff today.

Tony (14:08):

Oh, no problem. It was good talking. Thanks for having me.

Heather (14:11):

Yeah. Thanks for joining me once again. I appreciate it. That's all for today. Stay tuned for our next podcast where we'll be talking about vulnerability and disclosure policies with Roxy, our Vulnerability Management Specialist and Hurricane Labs' owner and Chief Technical Officer, Bill Matthews. Until then, stay safe!