XanGo
SANS WhatWorks in Intrusion Detection and Prevention

Exploring Passive Analysis and White Lists with XanGo

About XanGo, LLC

XanGo, LLC is a recognized category creator as the first company to market a premium mangosteen beverage, XanGo® Juice, to consumers worldwide. A delicious daily dietary supplement, XanGo Juice harnesses the nutritional attributes of the whole mangosteen fruit through a proprietary formula. Based in Utah, XanGo is privately-owned and powered by a global network of independent distributors. XanGo's expansive operations include the United States and numerous international markets such as Germany, Canada, Mexico, Japan, Australia and New Zealand.

About Brandon Greenwood

Brandon Greenwood, GSEC, GCIA, GCFA, GCIH, is senior security engineer at XanGo, LLC. His background includes network engineering and various security-related responsibilities although his primary focus is intrusion detection.

To come up from scratch on PCI compliance, XanGo needed a reporting tool that would show auditors a consistent history of logs. In addition, the new senior network engineer knew he wanted IPS capabilities for a planned expansion. The solution he found met those requirements and other features, like RNA's passive scanning, allowed him to get a solid baseline on network segment activity.

Interview

Q. Tell me a bit about your corporate network environment so people can get a picture of how you use the product.

A. We've got our corporate headquarters and a couple of other sites in the U.S.—and a few more in Asia. We're planning on expanding to Europe and some other places. We probably have close to 800 users total throughout those environments, the majority of which are here in the U.S. The environment is broken into a typical three-tiered environment; internal users are on different segments, separated by firewalls—just typical corporate infrastructure.

Q. Was there a particular event that prompted you to go out and look for Sourcefire?

A. Yeah, I actually had experience with multiple IDS and IPS vendors in previous jobs. This position was created for PCI compliance and part of PCI compliance is having an IDS in place to be able to meet that requirement. So when this position was created they said, "Okay, this is what we're going to do, we're going to use an IDS. We're going to make sure firewalls are set up, encryption is done." IDS happens to be one of the areas that I am very comfortable in. I've had many years working with Sourcefire® and other vendor implementations of IDS and IPS. One of the reasons for coming here was to start that phase of the security infrastructure from the ground up and being able to bring in what I wanted and what I thought would work best for the environment.

Q. So, you have a lot of experience with IDS vendors. Did that mean you didn't need to a lot of background research because you already knew which one you wanted?

A. Well, even though I have a lot of experience with IDSes and IPSes and the technology, I still wanted to get the right fit for XanGo. I still brought in you know had a bake off between products, mainly ISS, Sourcefire, and Cisco products. Not only because I wanted to see how they would work in XanGo's environment, but I wanted management to know, that I was taking due diligence on my part and not just coming in with the attitude of, "we're going to go with this because this is what I know." I wanted them to know that I was going the extra mile and looking at these other solutions and seeing if they would be a fit for what we have here.

Q. Did you already have something in place?

A. When I came in there was nothing in place. To kind of get them up to snuff and kind of have something in place for PCI I did deploy SNORT® sensors throughout the environment, but they just didn't give me what I was looking for with regard to reporting and some of the features that Sourcefire's RNA™ provides that I wanted in the environment. So we had the little checkbox that said, "Yes, we have an IDS," but you know, down the line we wanted to go with something that would give us the extra features.

Q. How did you decide which three IDS/IPS products you wanted in the bake off?

A. I went with the three that I've had the most success with. Like I said I've worked with a wide range of IDS/IPS solutions. I didn't want to bring in an IPS right away. I wanted the ability to move to an IPS once we got a focused environment down and could implement an IPS. But the three that I've worked with, felt the most comfortable with, and have had the most success with have been with Cisco, ISS, and Sourcefire and that's how I brought in those three.

Q. And so you do use it as an IPS?

A. Yes.

Q. Can you tell a little bit about how you feel that differentiates your network security from if you just used an IDS?

A. Oh, you're asking if we use the IPS feature now?

Q. Yes.

A. It is running on non-impact segments but I have not turned up the IPS functionality up for any customer impact segments right now. But we do have a server farm that we're getting ready to deploy the IPS feature set on. What I've done is instead of just going in guns blazing and turning up IPS and having any misconfigurations possibly bring down a service or having users not be able to get to a web page, I've gone ahead and implemented the IDS feature set on that segment. As I've tuned it, making it so we know exactly what traffic is going across that segment so we're not going to get any false positives or at least lessen the chances, I've created some custom signatures so we know only this traffic is going to go and made sure that the Sourcefire rules and signatures are giving us what we need. As soon as we're comfortable, and I'm pretty much there right now, we're going to go ahead and flip the switch for the IPS and watch it run.

"Instead of getting traditional IDS alerts and having to go and investigate to make sure the exploit that possibly came through was actually intended for a box that it could exploit, RNA says, 'You know what? There's an IIS exploit coming in against an Apache server and I see that as a lower risk.'"

Q. So you plan to use the IPS if this trial is successful?

A. Yes, in a focused environment like a web or database server farm. We'll probably still keep the IDS for umbrella situations where we have a lot of different users using a lot of different architectures because that's a lot tougher to tune to what is comfortable from an IPS perspective. But yeah, the database segment is where I plan on going next.

Q. How was the install?

A. Install was really easy. Of the three that I've worked with, Sourcefire was without question the easiest to get up and running and start configuring and start tuning. We had a terrible experience with the ISS product.

Q. What made it more difficult with ISS?

A. When installing the ISS product, I actually had to have their engineers come out multiple times to set up the reporting database that their sensors report back to, and I ended up having to ship the box out to their headquarters. They sent the box back telling me to go ahead and run it and I still had to have an engineer come out and do some configurations. I'm pretty familiar with ISS and I take pride in being able to set it up, but there's something about it that didn't allow for ease of set up.

Q. What set Sourcefire apart and made it easy to use?

A. Sourcefire just hopped right on the network. It was a matter of addressing the sensors and Defense Center, configuring the sensors as to where the Defense Center was, getting the pre-shared key on the devices and it was off and running. No further configuration. Then it was just a matter of going ahead and tuning the sensors and telling RNA what to look for. In terms of getting it up on the network; no issues.

Q. What do you think of RNA?

A. I love RNA. I like the idea of sensors, but RNA gives you a lot of information, gives you a lot of additional information that many IDS/IPS vendors don't necessarily give you right now.

Q. What types of information do you see?

A. Instead of getting traditional IDS alerts and having to go and investigate to make sure the exploit that possibly came through was actually intended for a box that it could exploit, RNA says, “You know what? There’s an IIS exploit coming in against an Apache server and I see that as a lower risk.” I like that feature.

Q. Is there anything besides ease of installation and RNA that sets Sourcefire apart from the other two?

A. As I was running the bake off I went ahead and created malicious traffic with Nessus and Metasploit, captured the traffic and included some other traffic in it. I tried to make it as noisy as I could and would replay that traffic against Sourcefire, ISS and Cisco. Sourcefire in my test caught, if I remember right, all of the exploits. Depending on the speed of the replay, ISS and Cisco had issues. I decided to see what it was like dealing with their tech support. ISS and Cisco both had pretty long hold times, but with Sourcefire, whether it was an e-mail or whether I called them direct, I generally got very supportive tech support right away.

> “I decided to see what it was like dealing with their tech support. ISS and Cisco both had pretty long hold times, but with Sourcefire, whether it was an e-mail or whether I called them direct, I generally got very supportive tech support right away.”

Q. Were they equally supportive after the testing?

A. Yes. I mean I’ve had hardware issues. I had drive on my Defense Center and they went above and beyond being able to help me troubleshoot that and getting a replacement out here.

Q. RNA offers a value add to the source and detection capabilities?

A. Right.

Q. RNA is also, in its own right, a passive scanner or a passive listener that provides some profoundly useful information. Have you used it to find if somebody stuck a rogue device on the network?

A. I have created a white list for separate environments. We don’t typically put it on the umbrella segment because so much goes in there. We’ve got these white lists defined for the different segments and if something changes we know about it right away and we’re able to at least question whoever put it in, whether it was just Admin or an engineer or whatever. So then we can say, “Hey is this needed?” And sometimes this was within minutes. We can either look at doing a task a different way or go ahead and create a pass for that traffic.

Q. Does it have a name in the Sourcefire family? It’s RNA, but does that particular function have a name? Is it a package capability or is it something you just did because you knew you needed to do it?

A. It’s something that I did because it’s security in layers. I mean just because we have the IDS doesn’t mean we shouldn’t be looking at this additional information. I mean if we can add an additional layer, then we should be doing it. If we’ve got the capability and Sourcefire provides us with these features that are a benefit to us from a security standpoint, then by all means we should be using them.

Q. What did you know about the white list capability and the sensing new devices? Did the tech guys tell you about it or was it just obvious to you? How did you know that that capability was available to you?

A. Just from reading the documentation. And I actually talked quite a bit with one of the Sourcefire engineers, Jason Billings, and he would say, “Hey, you’ve got to check out this new feature that’s coming out,” and as it came out I looked at it. It definitely is easy now. You just go in and tell it, “this is the segment, this is what I want to look for.” It is a no brainer.

Q. Does it also have the ability to tell you what's running on your system?

A. Yes, depending on what passive analysis was done and whether it sees that segment and whether it has the fingerprint. I could pull up a search and say "Show me any work stations running Mac, or whatever, and if it's configured to look at that segment and on that segment those exist, it will tell me.

We actually had another instance where working with RNA, not necessarily the white list, where we had actually set up some traffic flow trends and someone had brought in, against policy, a personal laptop. They put it on the network and were DDoSing sites in China and Brazil, if I remember correctly. We were able to identify that very quickly based on the flow was going over a certain percentage and take immediate action on that individual and box.

"We actually had another instance where working with RNA…we had actually set up some traffic flow trends and someone had brought in, against policy, a personal laptop. They put it on the network and were DDoSing sites in China and Brazil. We were able to identify that very quickly based on the flow was going over a certain percentage and take immediate action on that individual and box."

Q. Why was the guy doing the DDoSing?

A. What it looked like in the forensic analysis was that he was using IE, and ActiveX had been used as a vector to install an application on the box, and it went from there. After doing further analysis, I found that the box would go out and hit a site in the Philippines, pull down a list, the list would tell them boxes to DDoS and they would launch the attack.

Q. Is there any reason you wouldn't have it looking at all segments? Is it a price issue or a traffic issue or a capacity issue?

A. We've got it in house right now looking at all segments. Some of them are a little bit different. Some of them are tuned or some are under our umbrella as I stated to you earlier. Money and source space could also possibly be reasons.

Q. So when did that capability become available to you?

A. I didn't really start using it until I came here. I've worked with other organizations, big organizations, where I really didn't have a say as to what we were going to look at. We've had the product for about eight months or so.

Q. Was the capability in there two years ago? Could you have just turned it on two years ago or was it not even a capability you could turn on a couple of years ago?

A. No, I believe that it is fairly new and Sourcefire calls it "Network Usage Control" or NUC. It is their post-connect NAC and offers a series of menus and white lists and things like that so with just a few clicks administrators can change the way that they've got their compliance policies set up related to the usage of operating systems, services, applications, protocols, and so on. With it, I can identify policy and regulatory non-compliance. I can see which users are running unauthorized applications.

Q. If you don't have certain skills how much of the value of these tools do you lose? If you don't have the forensic capability, if you don't have the ability to really understand the attacks, how much of the value goes away?

A. If I had gotten this tool and I didn't have the skill set that I have right now, I'd still be able to look at a flow graph in RNA, and I would have still been able to see that DDoS attack going out on the graph. It's a huge spike or an out of norm based on a trend line or base line on my network traffic and it would have told me, "Hey, something's out of the norm here." And they could very easily look and say, "Hey, it's this box sending this many flows out which is not normal. I need to look at that box". And even though they may not have the forensic skill set or traffic analysis skills that someone else might have, they would still be able to get that box off of the network.

Q. And they could unplug it which is mainly the main mitigation that you want?

A. Correct.

Q. They wouldn't have been able to go out and find out why it was infected or what to do about it or how to get it cleaned out.

A. Right. But get it off the network and you're helping your organization out at that point. From there they could bring in additional help if they needed it.

Q. How much manpower do you think it takes to support Sourcefire in the ways that you use it?

A. Well, I'm really the only guy here that does security at this level. I mean we've got network engineers and sysadmins, but what I do with Sourcefire is I typically spend two hours a day, doing just routine things, looking at logs, updating signatures, maybe if there's a patch for the engine, things like that.

Q. Okay, how much background did you need, whether it was from training or experience or something that you've learned, to be able to use Sourcefire effectively?

A. I've had a lot of training. To the level that I use it, I have not taken any of the Sourcefire training that we got as part of the package. I plan on doing it. But, I've got network administrators who all look at the alerts right now and even though they probably can't tell me why they're seeing this type of traffic, they're able to see if there's a problem.

> "Sourcefire calls it 'Network Usage Control' or NUC. It is their post-connect NAC and offers a series of menus and white lists and things like that so with just a few clicks administrators can change the way that they've got their compliance policies set up related to the usage of operating systems, services, applications, protocols, and so on. With it, I can identify policy and regulatory non-compliance."

Q. So the average person who can sell security can detect a compliance violation and can pull a box off. How do you know specifically where that box is?

A. I think you've got to have an understanding of the environment. Basically, if the network environment is set up in such a way that if you know a certain network or network range, in maybe this building or this location, or you can go back and go through your switches and find out where those are at, you can find where it is physically.

Q. So he has to have a map somewhere?

A. You'd have to have a map or go through routing and switching just to see where that box might be. Or if they know where that switch is, follow the MAC back and say, "okay it's coming off this switch, I know it's over here." Or if you've got DNS and you're getting an IP address, for instance an address going to this box in Japan or maybe naming standards indicate that this is in Japan.

Q. Gotcha. So you use naming standards as part of the map?

A. Yes.

Q. What's the value add that your skills do? It's the understanding of why it happens, right? How and why?

A. Yes.

Q. And it's a combination of your IDS and your forensics knowledge, right?

A. I think it's a lot of different things. You know, just being familiar with the space of how networking or information security is and having worked in it for a while. I think you bring all your experiences to the table.

Q. I want to try to begin to emphasize the value that the security person brings to these things because there's a little bit of a marketing pitch of just turn it on and it will find things and life will be good.

A. Yes, that can happen.

Q. When I've seen that and in fact, nobody looks at it. There's a compliance rule and they point to it and say, "Look that's the way we do compliance." And you say, "But what have you ever done with it?" And they say, "Well, I don't know. Nobody really understands it."

A. Sourcefire, I believe, can go out and look at a segment and it will tell you what boxes are out there and what services RNA has detected and you can go from there to set up compliance. So if you are just a network administrator and you don't know 1521 is for your Oracle, for example, you just say, "okay, I see these reports running on these boxes, why don't you research what that is, okay, yeah I need that, I don't need any of these other ones." It would make that type of job a lot easier for someone who maybe didn't have the skill set. Had I not had a particular skill set, I probably would have used it like that.

Q. And why don't you, if it's easier?

A. Because I want to know first of all through RNA what's running right now, but I also want to know from a policy perspective what should be on that segment. So I want to say, "You know what, this box in this segment should only have, for example, 1521, no Web, nothing else." I can say I should only see this and if anything deviates let me know and I'll flag it as positive or we'll create that as part of the white list. I want to start with the base and that was my way to approach it.

"You've got support forums, not only from Sourcefire, but if you're working with signatures or something with Snort, you've got the entire Snort community you can fall back on. Maybe you've got an issue that you don't want to bring to Sourcefire, you know, 'how do I create this regular expression looking for this?' You can put something out on a forum you'll get the answer relatively quickly."

Q. How do you know that Sourcefire improves your security?

A. It's improved our security, I would say, in more ways than just security alerts. We get a lot of other information like misconfigured networks that could be a security problem.

Q. How often do you use it to run reports and go through audits? I know the focus you have on PCI compliance so you're probably doing it pretty regularly.

A. Yeah, reports are typically run once a month for senior level management. They generally want to check status on where we are with security in general. So those are run once a month and at the end of the year we run it for the PCI auditors. We can say, "here are our monthlys, our yearlys," if you can go back that far in your database. Our information for the yearly was only five or six months old.

Q. What do you think about the information that's in the reports? Is it really comprehensive or are there things you wish it had?

A. You can make it pretty comprehensive. There are typical management styles where you just give them three or four pages, just kind of an overview, but you can get pretty granular with your reports as well. If you had an engineering team or a security team where you maybe had different levels of IDS analysts or even firewall guys, you could say, "You know what, here's what I'm seeing." You could print out these reports and say, "Hey, let's take a look at this." So there are some pretty good reports and features you get out of them but there are also some other things I'd like to see with the reports that probably aren't in there right now.

Q. Are there any other features that you wish Sourcefire had that it doesn't?

A. There's one piece that I wish it had, but really no one has right now. I had to bring in a third party solution to kind of get a feature set. Sourcefire, ISS and Cisco didn't really offer this, but with Sourcefire and a third party product, if an alert is generated and I want to see that entire packet, I can tag that alert and grab that entire session. It's important to be able to look at the entire flow and maybe where else an attacker may have tried to hit inside the network—full content data versus just the alert. It watches the same segments that Sourcefire is watching and if I get an alert or something is generated, I can go back in time, pull up informational statistics.

Q. How do you feel about Sourcefire overall?

A. I love it. I've used them in my previous couple of jobs and here and, in my opinion, it's the best IDS that I've been exposed to. You've got support forums, not only from Sourcefire, but if you're working with signatures or something with Snort, you've got the entire Snort community you can fall back on. Maybe you've got an issue that you don't want to bring to Sourcefire, you know, "how do I create this regular expression looking for this?" You can put something out on a forum you'll get the answer relatively quickly.

SANS Bottom Line on Sourcefire at XanGo:

1. **Aids in PCI compliance by providing an audit trail;**
2. **Passive scanning by RNA immediately shows rogue devices as well as identifying vulnerable systems;**
3. **Requires little manpower;**
4. **Provides post-connect NAC which can be used for compliance enforcement even by those with fewer security skills and training;**
5. **Very responsive technical support.**

About SANS What Works

SANS What Works saves user organizations months of time that would be wasted in trying to uncover the truth about which Internet security tools actually work in their environments. What Works is a user-to-user program in which managers from organizations that have implemented each of the effective internet security technologies tell a complete story of why they deployed it, how it works, how they know it actually improves security, what problems they faced, and what lessons they learned. Without What Works, buyers are at the mercy of sales people who, too often, do not have sufficient security expertise to understand how their products fit into a defense in depth and what the tools can and cannot do. Only users know the answers to those questions. Smart buyers have always demanded an opportunity to talk to users directly. SANS What Works brings those users to you in written interviews and in live and recorded webcasts where you can get your questions answered.