Hello, I'm Roger Safian. Today is Thursday, December 8, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

Today’s podcast is going to be on a lot of frightening stories, one might say. You know, I’m always talking about I think these stories may be blown out of proportion a little bit by the press, seems to be kind of a common theme sometimes in security, the way that they use the language to express some of the stuff, I don’t necessarily think it helps us. Anyway, today, recently I ran across a story that I thought was just like, oh my God, I hope they’re blowing this out of proportion, and I’ll actually include a link to it. It was “Man-made super-flu could kill half humanity”, and they want to know whether or not they should publish this data online. My assumption, of course, is that you can’t just whip this up in your backyard, but who knows. Anyway, I guess when I’m looking for a new standard of blowing things out of proportion; I guess I’ll have to compare it to that.

Anyway, let’s talk about some 0-days that are out there. There’s a bug in Adobe Reader and Acrobat right now, and there’s not a fix for it, so if you are using Adobe Reader and Acrobat, you probably want to be a little careful, maybe think once or twice before you click on documents that you’re not familiar with, especially on websites, and my guess is that’s likely where you would run into problems. There’s supposed to be a fix for Windows by December 12, and they’re saying January 10 for Macs and older versions of Adobe Acrobat and Reader. Not a good situation, but as you know Adobe gets hit quite often, so keep your eyes open when the new version is out for your system, go ahead and grab it, and I’ll try to make a reminder when that happens. While we’re talking about, there’s a bug in Yahoo! Messenger that can basically allow somebody to take control of your Free/Busy, the status indicator you’ve got on there. I don’t know how important this is, I’m not a Yahoo! user and I don’t usually use these kinds of tools anyway. There’s not a fix for it yet, but hopefully that’ll be out there soon. Any time you have issues like this, I think it’s incumbent upon the vendor to get out there and fix it as quickly as you can, and I hope that’s true for both of these here, and I’m relatively sure that it is.

I did find a story about hacking XBoxes, and I thought it was kind of interesting because basically what happened to this guy, the author of the story, is his XBox Live account was taken over, and he basically wrote a story about it, “hey, here’s what happened”. That’s kind of interesting and kind of surprising too that Microsoft can’t do more to stop this kind of stuff. And I’m not saying stop the stuff, you know, I don’t know how his account got hacked. That’s probably difficult to do. But what they do is they allow purchases to be made, and then those
purchases to be sold to other people and turned into money, and it seems like that part of the transaction, Microsoft could do something about. Maybe they are, maybe I don’t know enough about it, but really I’d like to see more done around here because I think a lot of the bite out of cybercrime would go away if there was just not as much money available.

And while we’re talking about cybercrime and money, we’ve got the report here from Booz Allen about the top 10 cybersecurity threats for financial services, so it’s not necessarily your everyday user, but a lot of the stuff that they’re talking about is stuff that we’ve talked about before, growing threats that have to do with mobile devices, things like that, so I’ll put a link to the article, you guys can take a look at it, because it is kind of interesting, and I think it’s kind of interesting to compare something like this here, which is directed at one specific sector, versus something that’s more broadly based.

And then the last two stories that I have here are, one is about - remember I talked about blowing things out of proportion - the title of this story is “Millions of printers open to devastating hack attack”, and what they’re saying is they could give the printer instructions so frantic, this is a direct quote, “so frantic that it could eventually catch fire”. Now, you know, my guess is maybe it’s possible, but it certainly seems out of the realm of probability. Hewlett-Packard, who this was directed towards, says this is definitely not the case. They did issue a patch for this here, and this is a problem, and I think part of the problem is it depends on how you’ve got your printer installed. Printers shouldn’t be on the network unless they’re behind some sort of firewall. I don’t think that the printer was ever made to just be sitting there on the open Internet so that anybody from anywhere could get to it. That seems like a bad thing. And it seems to me like if you’re taking reasonable precautions here, you’ve got your printer on the network, it’s behind a firewall, it’s limited to your specific range of addresses, you’re probably OK. Hewlett-Packard does have a patch for some of their printers; my understanding is they’re working on more. Whether or not this is more widespread I can’t tell, but you’re certainly going to want to take and download the updates for your printers. At least take a look at this article here so that you can see which printers are potentially hit.

And then the last story that I want to talk about seemed to be just everywhere when I got back from vacation, and that is, there’s a company called Carrier IQ, and they seem to be on a wide variety of smartphones, and they essentially are monitoring what happens on a smartphone to provide information to the carrier so that they can fix problems or know what applications are really popular, basically improve your experience. But what it looks like, at least from a video that was posted on YouTube, is that they are getting way too much information. It’s possible they may be getting information like your bank account, passwords, all sorts of stuff, and they’re just logging a tremendous amount of information. Now what they’re doing with it and what information is being logged varies, and certainly nobody seems to be in agreement.
There’s lots of stories about this, there’s already several lawsuits that have been sent against it, companies are already saying they’re going to remove the software; Apple, for example, is going to remove this software from their phones. I wouldn’t be a bit surprised to find out that this sort of behavior is going to trigger a change in the way that these phones are used and the way that software of this type is used. If I had to make a prediction, I would say this company’s probably not going to be in business that much longer. It seems like when something like this happens, the markets react pretty quickly and snuff them out. Certainly, that’s true in the first couple of cases in any kind of a new thing; we’ll have to see what happens here. You can turn this stuff off, and I would encourage you when you get your phones and you’re activating them, or for that matter a computer even, they always ask you, “Do you want to participate in this here”, and you get an opportunity to opt-out of these things. Now I think it should be opt-in, but unfortunately a lot of these things are opt-out, but, you know, opt-out. Say no. You can always go back and turn it on later if you really think you need to give them some sort of information, but say no. It would be interesting to see how this all shakes out. We’ve got the US Senate want to take a look at this, the Europeans are involved, they want to take a look at it to see if their privacy laws have been violated, the FBI is looking at this, they want to know if data protection laws have been violated, there are people who say “Look, they’re capturing a lot of data, but they never send it off the phone”, there are people who say they do send it off the phone, there’s certainly a lot happening here. What I would say is, I’ll post a link to several of these stories on the website and you can take a look at it, but if you do have one of these, you might want to check your phone and Carrier IQ and see how you can disable it on your phone.

Anyway, thanks for listening. If you have any comments or suggestions, please feel free to send them to r-safian@northwestern.edu, and as always you’ll find additional security information as well as the notes that contain the links for today’s podcast at our website www.it.northwestern.edu/security/.

- Information Security News Podcasts Archive
- NUIIT Home