Transcript: NUIT Information Security News Podcast, September 15, 2011

Hello, I’m Roger Safian. Today is Thursday, September 15, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

Just a small note about last week’s podcast: Microsoft released their patch information early last week, and so the links that I put up for the Microsoft Security Bulletin, those were correct, but for several days Microsoft took it down and then put it back up, so if you tried getting a hold of that information last week and the link didn’t work for you, I apologize. It’s not necessarily my fault, but I guess is my fault, so sorry about that, but the link is still up there, and it still works, so if didn’t get a chance to look at that Security Bulletin, feel free to go back to last week’s podcast and grab that link.

And then while we’re talking about updates here, there’s new versions of Adobe Acrobat and Reader. Those just came out the other day, so, again, make sure you grab that, especially things like Reader, as it just seems like that’s being used in so many exploits lately. Adobe’s really been having to work extra hard to keep their product up to date. So grab the latest version of that. It should, if you’ve got the most recent version, it should update itself automatically, but if it hasn’t done it yet, you can just go over to the Adobe website and download the updates manually.

And then I want to talk a couple stories here that I saw that, I’ve mentioned this before, I think sometimes the press kind of blows things a little bit out of proportion, or antiviral vendors or security vendors maybe blow things a little bit out of proportion, not that they don’t have a story there, but I think they have to sell it in a way that - there’s serious issues to be worried about, and then there’s issues that are maybe not as much of a concern. So these two stories I feel fall into that category. And one is, the title of the article is called “Malware Burrows Deep into Computer BIOS to Escape AV”. And this is a serious issue, no doubt about it, but it’s limited to a handful of machines that are produced in China. It’s not widespread, I don’t even think it’s necessarily that useful for the malware folks, I mean who knows what they’ll make of this here. But, in this particular thing - I guess I should back up a little bit. Just in case you don’t know, the BIOS is what basically starts up your computer. And so the idea is here that what they’re trying to do is interject the malware at a point where the computer - let’s say you’re running antiviral software, it’s got no chance to do anything, do anything to help you stop the infection. So this particular piece of malware is called Mebromi, and it’s, as I said, it’s just in China, and it looks
like it’s confined to the Award BIOS. You know, I just don’t think this is a lot. So my sort of beef here is not that it’s being reported, I’m all for that, but let’s put things in perspective a little bit.

Here’s another one of those stories: “QR Tags can Hide Malicious Links, Experts Warn”. Well no kidding. You can have a malicious link just about anywhere. Now do they want people to stop using QR tags? That’s just not going to happen. Now the one thing that they said in this article that I think made sense is, look, be careful, if you’re clicking on a QR tag and maybe it’s been covered up with a sticker or something like that, so it’s not - you know, you buy a bag of potato chips and there’s a QR tag on it and, you know, if it’s not the one printed by the manufacturer, maybe be a little extra cautious or maybe don’t just, you know, you see some QR tag on a 8 and a half by 11 piece of paper that’s hung up on a bulletin board. Maybe you don’t go there. Take the same sorts of precautions with these tags that you would do with any other links. And, let’s just leave it as that. So, it’d be interesting to hear what you have to say about this. If you have any comments, drop me a note and I’d be glad to hear what you have to say.

Now let’s talk about something that I do think is a real risk, and that’s mobile banking. And I’ve talked about this a lot, and I’m probably going to keep on talking about it because I think it’s an issue that we brought up very early and that a lot of people are coming around to say that this is truly a problem. So I’m going to post a link to a couple of different articles here along these topics. One is called “Mobile Banking: The New Risks”, and they’re not new risks if you’ve been listening to this podcast, so give that a read. Another one, though, is malware for the Android phone that basically is looking around to wait for you to do mobile banking, and then it’s going to try to hijack your credentials, basically send you to a site that you think is your bank, but in the middle is going to be sending this malware site that’s going to be able to get a hold of your banking information. You know, I’m just not a big fan of mobile banking on whatever device you’ve got. Maybe it’s different if you’re using your computer at home, but you really want to be careful, even with your laptop, if you’re at these mobile hotspots or you’re at Starbucks or any of these types of things, you know, banking information is something I think you need to really be cautious about. I know it’s really convenient, but you need to realize that once somebody gets a hold of that money out of your bank, it’s going to be a real pain for you, so you’ve got to be very careful there.

And then we’re going to close up with a story on Facebook. Now Facebook’s been making a lot of changes. I don’t know if Facebook is doing these in response to Google+, but some of the changes that they’ve been making look kind of Google Plus-y, you know, they just released another one today where you’re going to be able to kind of set up Groups, looked very much like Circles in Google+. Anyway, one of the changes they made recently allows you to decide whether or not you want a photo that you’ve been tagged in to show up on your Newsfeed or your Wall. It gives you a chance to say yes or no beforehand. And I’m going to post a link to this
article so that you can turn this feature on yourself if you want. Personally, I think this is a good idea. People can put up photos and tag you in them, and you don’t necessarily have to be in a photo in order for somebody to tag you in it. I mean, I’ve seen photos where people just tag hundreds of people by their names because they’re hoping that they can get friends of these people to look at this. Or maybe it’s a photo that you don’t necessarily want to be tagged in. So yeah, I think this is a great feature, and I encourage Facebook to do more stuff to allow people to control their own privacy.

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