Hello, I’m Roger Safian. Today is Thursday, September 22, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

One update that I want to talk about real quick is an update to the Adobe Flash Player. A lot of people are probably using the Flash Player, so make sure you grab the update. I’m not sure if this is going to update itself automatically; I unfortunately, before I tested it, I did the update so now I’m not sure if it’ll do it automatically, but don’t take any chances. Flash is something that is targeted pretty well, so you’re not going to want to let that happen. I’ll post a link on the website to an Adobe page so that you can test your version of Flash to see what it is, and it’s quick and easy to update it if you’re not running the latest version.

While I’m doing that though, I want to take just a moment to trash those people over at Adobe for putting the checkbox on “Install Google Chrome” at the same time that they’re doing their update. I don’t have anything against Chrome, and I don’t have anything against them offering to install it or making software available as part of this update. That’s great. But don’t put the checkbox on there by default. There’s going to be a lot of people that are going to install Chrome, and they’re not going to use it, maybe they won’t be updating it, maybe it’s just sitting there with a vulnerability on their system at some point in the future. If you’re listening to this and you’re from Adobe, you are definitely off my Christmas card list.

Then I want to talk a little bit about an article that I read on the Register about exploiting weaknesses in SSL. And I think this is pretty serious; I don’t think it’s serious enough where, you know, shut down the web and go live in a cave yet, but it’s something that worries me. Weaknesses in SSL have been known for quite a while. There are other versions of software out there that would work better. I should say SSL’s got newer versions; there are things like TLS, but they’re just not being supported yet by the browsers. And at some point, people have to start using this stuff. We can’t always rely on the older technology - it’s great if older technology works, but very often there’s known weaknesses with older technology, and newer things come out and you want to replace it. So I encourage the vendors out there to make sure your browsers support the newer versions of encryption, and then also make sure that if you’re running a website, that where possible you use newer versions of encryption as well. Now, this particular vulnerability, I don’t necessarily know, as I said, if it’s the end of the world. It would take about 30 minutes, according to the article that I read, to decrypt a cookie. And, you know, while that’s not necessarily a good thing, it’s not the end of the world. 30 minutes is still a fair
amount of time. But I really do hope that this is, for me, that what is important about this particular story was it’s a wake-up call to everybody that, “Look, SSL - great, but it’s run its course, and there’s newer stuff out there, and let’s start using the newer stuff”.

And while we’re talking about newer stuff, there was another article that I read on the Register, practically at the same time, and it was, “Skype for iPhone Makes Stealing the Address Book a Snap!” And basically, what it boils down to is, the iPhone and iPad decision was made to make the Address Book available to every application. Now, is that a good idea? Yes, no, I don’t know, I guess it’s debatable. My personal preference would be, it would be nicer to have, maybe the user’s given a choice what applications should have the Address Book available. Likely, Skype is an application that I would want to have my Address Book available, but who knows, right? Anyway, that’s one weakness. The other thing is, on the Skype end of things, they don’t do any sanitizing of what you’re passing it, so you can pass them just about any crap, and it’s going to be run. That’s not a good thing, so I hope that Skype will look at how they’re running their system. I also hope that Apple might reconsider maybe not having the Address Book available to every application that’s out there. And again, this isn’t necessarily the end of the world. You know, person’s going to send you a malicious chat message, for example, with a malicious code. You might even recognize this when you see it, you might not, I didn’t get a chance to see what it looked like, but my guess, most people, do they accept chats from people that they don’t know? I don’t, maybe others do, who knows. I would just say be cautious out there though, especially if you’ve got things in your Address Book that you might care about.

And then I wanted to talk about Microsoft put out some statistics about cleaning up the Zeus bot. If you’re running a Microsoft system, one of the things you do almost every month is you run their Malicious Software Removal Tool. And I think this is great, that when Microsoft does their updates, they also look to see if there’s known problems with your machine, and they just sort of clean it up all at the same time, and that’s outstanding. What I think is interesting, though, is they put stats out there for the Zeus trojan and how many times they’ve removed it. It varies, but it’s been as high as 113,000 in a single month, and the low has been 60,000. So, if you’re removing somewhere between 60 and, say, 110 thousand infections a month, that’s a lot. That’s something to be concerned about, and I would be very curious to know, that when I saw this stuff, the very first thing I wanted to know was, “I wonder how many times they’ve removed the same infection from the same machine because they clean it up and the person goes right back to doing what they’re doing and gets themselves infected again”. Anyway, though, I do want give some pat on the back, a thumbs-up to Microsoft here, because at least they are trying to make a difference by cleaning up these machines, and that’s a good thing.

And then I want to close with a story here that’s got a title that’s a little on the edgy side. The title of this article is “How to Stop Pervs from Stealing your Naked Pics”. And I’m not necessarily
interested in providing any advice along this line. But what I thought was really interesting about this article was it was filled with great, practical information about how to protect you online. It’s really, really good stuff, so I would encourage you, regardless of what sort of pictures you may be taking, just to take a look at this article, because the information that is available is information that you could use for just about any circumstances online. And I should say it’s not on some creepy website; this was on MSNBC, so it’s, you know, I’m really glad to see this kind of stuff, especially since it does seem there’s a rash of this naked pictures being posted around on the internet. In fact, I think somebody speculated that eventually there’s going to be naked pictures of everybody on the Internet. I hope not; nobody wants to see me naked.

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