Hello, I’m Roger Safian. Today is Thursday, September 1, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

Our first story is about updates to Mozilla’s Firefox. There’s a new version out, fixes some security holes, so, what we pretty much say every week, you’ve got to go grab the latest version, so if you are a Firefox user, go out and see if there’s a new version of Firefox. It may have updated already, but it doesn’t hurt to double check. And while we’re talking about updates, there’s a new version of Ubuntu. And my guess is probably not a lot of people are using Ubuntu, but you may be using it and not realize it. Ubuntu was pretty popular on netbooks, so if you’ve got a netbook lying around or a netbook that you’re still using, it’s possible it’s running Ubuntu, and you might want to make sure that you grab the latest version of that to make sure that you’re safe, because, as we’ve said before, when these vulnerabilities are out there and they get fixed, the bad guys know they’ve only got a limited window before they’re not going to be able to take advantage of this, and the attacks definitely increase.

And then I want to talk about a campaign that’s being done by the Department of Homeland Security, but it’s also partnering with universities, the Boys & Girls Clubs of America, and basically it’s called “Stop, Think, and Connect”, and the idea here is getting people, especially younger people, to think about computer security. Now I love this. I mean, I don’t know if the program will work. I just like the fact that there’s somebody out there trying to do something, you know, put a program together that people, regular, everyday people can make some sense of, because I really do feel that computer security is very important to computer security people, but beyond that, it’s not. And I’m not necessarily saying that’s a bad thing; you have a computer, you want to use it to do your work or have fun or whatever. You didn’t buy this computer so that computer security could consume your life, so I think we have to work on making things simple, but at the same time I think we have to make sure that people understand what the problems, what the risks are out there and know how to properly protect themselves, so I’m glad to see this. I don’t think we’ve got anything planned for Northwestern specifically with this campaign, but if we do I’ll make sure to include it in the podcast so that everybody can know about it.

And there’s a new Windows worm going around. Now I’ve seen a few cases here on campus. This is called Morto. It’s got a few other names as well, but basically what this is is a vulnerability that’s going to attack you if you’re using remote desktop and you have a weak password. Now, Microsoft published a list of passwords that this is using, and, boy, they’re terrible passwords, I hope none of you are using them. But my suspicion is, rather quickly, this
password list is going to be updated because I just can’t imagine that that would be that big of a deal, and there’s much better lists out there. So you’ll find that even if your password’s not particularly weak but maybe just not very good, maybe you’ll get hit, maybe there are other things going on here, there’s some news but there’s a lot of information that turns out not to be true about this, so it’s the kind of thing I think we’re going to have to watch and see how this develops. But definitely, if you’ve got remote desktop, it’s really important that you make sure that any of the accounts that are on that system have good, solid passwords. Choose a password that’s longer and stronger, and then you don’t have to necessarily make it very complicated. You could just choose a password like “Today is the first day of September.”, and that’s a pretty strong password right there. There’s some special characters in there, and it’s definitely worth doing. I’ll post some links to the Morto information that I’ve got, and you can take a look at them and decide what you want to do.

And then the last thing I want to talk about was a story that came out of DefCon. And it had to do with home routers and universal plug-and-play, and basically what it is is it was reported that on home routers, the person at DefCon said he identified 150,000 potentially vulnerable devices, so my guess is it’s probably my router and your router and everybody’s router, probably other devices that we’re using at home too. Sort of the skinny is, plug-and-play was supposed to be used on the local network so that you could plug a printer in and your computer would recognize it. But not on the Internet, on the wide area interface, and it turns out there’s a way to exploit this on the WAN interface. Now, it’s possible, depending on what router you’ve got, you can disable this universal plug-and-play on the WAN. I’m going to post a link to an article that has some information, and hopefully that will at least answer some questions. I wouldn’t be surprised, though, if you give this a little time, that the vendors will come out with updates so that you’ll be able to patch this - I hope that’s the case - but it sounds like it’s the kind of thing that should be disabled. I don’t know why they would’ve enabled it in the first place, but I’d like to think they had some sort of good reason.

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
- NUIT Home