Hello, I’m Roger Safian. Today is Thursday, November 10 - happy 236th birthday to the United States Marine Corps - and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology. It’s going to be a short newscast today. I’ve got basically only two stories that I want to talk about.

The first one is updates. It seems like just about everybody had something to update in the last week. The Microsoft updates - it was patch Tuesday, so we expected to see updates from them - there were a lot of updates, I thought. It actually took quite a while for my machine at home to get updated. I’m not sure; maybe it was just because I was one of the first, or a lot of people grabbing them, you know, just allow a little extra time, is what I’m saying, for these updates to be applied. Apple released updates including some pretty important Java updates that need to be applied. And then Adobe put out updates. Firefox has a new version of Firefox, so if you’re a Firefox user that fixes some security holes there. So it seems like no matter what you’re doing, there’s a pretty good chance that there’s a new version of some of the software on your machine this week, so make sure that you grab those updates so that your machine can be nice and safe.

And then I want to talk about this “Operation Ghost Click”. This is a story that came out yesterday, and basically what it boils down to is the FBI and INTERPOL, I guess, have busted a ring that was infecting a variety of different machines. And they were using something called “DNS Changer”. Now we’ve actually seen this, and we’ve seen this software for quite a while on the university campus, and what it would do is it would change your DNS server to be a site in the Ukraine or some place like that. And so what we would - what I should say is if you look at your DNS information on your machine - PC, Mac, doesn’t matter - you should see an address that has something to do with Northwestern. Typically, those addresses would start with 129.105, or 165.124. This would change it to an address in the Ukraine, and what it would do is it would work just fine; your machine wouldn’t appear to be doing anything wrong. But what would happen is, let’s say you would go to Chase to check your bank account; it would send you to a site that looked very similar to Chase, and they would use that then to filter out your money. And that’s not a good thing. These types of malware can be pretty tough to deal with, especially because, as I said, for most people, it looked like their machine was working just fine, and in fact the way that we typically found infected hosts here at the university would be we would block these rogue DNS sites, and then peoples’ machines would quit working on campus when they tried going off campus, but they would work at places, you know they go to Cosi or
they go to Starbucks and their machine would work just fine. That’s this rogue DNS stuff, and it’s been out there for a while. I’m glad to see that these governments have gotten together and cracked down on this. They said that they were pulling 14 million in income, which I don’t know if that’s annually, which is not as much as I thought it would be, or is that monthly or daily or who know how much. Basically, they arrested some Estonians that were doing this. They’re on the lookout for a Russian who’s doing it. These DNS servers were pretty much all over the place but primarily in the former Soviet Union there. They estimate 500,000 machines in the United States were infected, and the figures that I saw, 4 million total worldwide, so that’s quite a bit. I’m going to post some information here from the FBI’s website on our links section, and then I’m also going to post some information from Trend Micro and a couple other places so you can look at this. I was hoping to find a tool that you could just run and it would say “Ah, your DNS information isn’t quite up to snuff”, but I can’t find that. The FBI does have tool where if you put your DNS server’s IP address in there, they’ll tell you if it’s involved in this Operation Ghost Click. Unfortunately, I think for a lot of people, that’s pretty tough. The FBI and Trend and some other places all have information on how to get your DNS information out and put it in there, but again I think just for a lot of people it’s probably more than they can do. But give it a whirl. Take a look at this stuff, and please try to be very cautious about these kinds of attacks because they can be pretty devastating because they are gonna try to grab your money.

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