Hello, I’m Roger Safian. Today is Thursday, January 5 - happy New Year everyone - and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

Our first story today is from Microsoft, who released an out-of-band patch last week. And basically what this is is, if you recall for your Windows operating system, they will release the patches for Windows once a month. Typically, this is on the second Tuesday of the month. So you’ll always see that regular updates of the Windows operating system, and that’s great. But every now and then, there’s a vulnerability that they feel is really important and needs to be addressed right away, and when that happens they release what they call an out-of-band patch, and they’ve done that, last week they did that. They don’t do it very often, two, three, four times, some number of times a year, so it might just be a little unusual when you see it updating at an unusual time. Don’t worry about it; that’s expected. In this case, there was a problem in ASP.NET, and Microsoft fixed it, hopefully before it caused any problems for you or anyone else. And actually, I applaud Microsoft for paying attention to these things, in this particular case, seeing that a problem was potentially serious and needed to be fixed before the regular patch cycle. I know it’s extra work for them to do that, and I’m sure all the Windows users appreciate that.

The US-CERT sent out a warning too about a vulnerability for wireless routers. And basically what happens is they did some research - one of their researchers put something up on his blog - that basically shows, “Look, the WPS-enabled Wi-Fi routers”, of which my guess is probably most of the people listening to this podcast, that’s what they have in their home, “they have some vulnerabilities and could easily be cracked with some simple tools”. Now, I think this is pretty serious, there’s no doubt about it. On the other hand, probably for most people it’s going to be a non-issue, and what I mean by that is, if somebody wants to target you, then certainly they’re going to be able to do that and they’re going to be able to probably get a hold of your router. There might be things that you could do to sort of stop this. All of them are sort of distasteful. One thing that you could do obviously is turn your router off when you’re not using it. You’d obviously save a little bit of money that way because you don’t have to pay the energy cost for it, but there’s a real convenience factor that you’ll lose out on. I’ll leave it to you to weigh the risks versus the benefit of doing that. You might be able to do things that might prevent it, I’m not sure, but you could try using MAC address filtering for your router and things of that nature. My guess is it probably wouldn’t help. You might try stepping up the logging on your router. Both of these things, the MAC address filtering and the stepping up the logging,
would probably only really be useful after you’d been compromised. You know, this is the kind
of thing that I don’t know what we’re going to have to do except rely on the fact that the router
manufacturers are going to address this, but the problem that I have with that is even when the
router manufacturers address this, how are they going to get that update out to all of these
routers out there? Remember, we’re talking about millions of routers. You know, think about it:
when was the last time you updated your router? Every now and then I’ll see something from
my router and I’ll go up and I’ll apply an update. But it’s pretty rare. The router doesn’t do
anything typically, like say your Windows or your Macintosh computer, that would go out and
update itself. So that’s a big issue there, so I’m not exactly sure what’s going to happen here,
but we’ll keep an eye on it and we’ll certainly let you know if there’s some change.

I did read an interesting story about skimmers at a grocery chain. Now we’ve talked about
these before. Skimmers are those little devices that typically they’re put on the face where you
put your credit card or your ATM card into a machine - you know, there’s that slot that you
slide the card into - and a skimmer is a device that’s put in front of the legitimate interface for
that card, and it also captures the information on your card’s mag stripe. Now what it turns out
is, at a California store, somebody had attached a skimmer to one of these instant checkouts -
you know, you go there and you just check yourself out and put your credit card in and you pay
- and that doesn’t necessarily surprise me. I hadn’t heard about it before, mainly been focusing
on this when it comes to ATM’s, but I suspect that we’re going to see these skimmers just
showing up in so many different places. You’re really going to have to be cautious about where
you put your card in. And again, what I would recommend you do is, before you put your card,
any card, into one of these devices, just give it a good look, and if you want to be extra safe,
grab a hold of sort of the front, where you slide your card in - usually there’s like a protruding
part, you know, you can grab that - if you pull it a little bit, if it’s a skimmer, it’ll probably come
right off. If it’s not, you’ll be safe - person standing behind you might think you’re crazy, but
hey, that’s the risk that one has to take in order to be secure. But, you know, just be aware. I
mean, these things are happening. It’s very easy to skim the credit card information, and very
often what they also do is they put in a little camera or something looking down so they can
maybe capture your PIN at the ATM machine. When I see more things like this, I’ll be sure to let
you know so that you can have one more place where you can worry about when you’re using
your credit cards or ATM cards.

And then, another story that really caught my eye here, and this is, a court reporter, this person
lost their records for a trial, and the person was convicted wants a retrial, and judges said, “OK,
we don’t have any records, we’re going to have to give you a retrial”. And this happens to be
for a murderer. Now this is pretty serious; one would think there would be really excellent
backups done for these kinds of devices, those little court reporting devices, but apparently
that’s not the case. Some foul malware came on, I guess it’s the computer that was doing the
backup, and wiped all this data out. This is pretty serious; if you’re going to rely on these kinds of devices, you’ve got to make sure that the backups are absolutely foolproof, because you can’t have, in this case, a murderer being given a retrial simply because of a technology failure. This is pretty serious, and I really hope that this gets addressed, because to me, this is kind of frightening.

And then the last story that I want to talk about, and it’s probably a big one, is the STRATFOR compromise. And we’ve talked about this the last couple of podcasts, and basically this is another one of these Internet companies, and they provide research, reports, things of this, and people have given them their credit card information and set up accounts and things like that on there. It’s no different than any other Internet compromise that’s out there, with possibly the exception of its clientele might be, in other words, instead of just Joe, Ma, and Pa, who are using a service, this might be more of a higher-end clientele, let’s put it that way. And it looks like the information that’s coming out keeps getting worse and worse, and this is probably pretty typical of these Internet break-ins, it just keeps getting worse and worse. Right now, it looks like a total of just over 73 thousand credit card numbers have been released online, and it looks like log-in information for another 860 thousand users has been released as well. Now, what’s bad about this is people have started doing some research on the passwords that people are using, and every time this comes up, it’s the same thing. People choose horrible passwords. Now what’s particularly bad about this is it looks like this is, as I said, it’s a higher-end clientele, they’ve got serious stuff to protect, and yet they’re choosing really bad passwords. So, for example, it looks like one of them is a high-ranking CISCO employee who just used a date, probably that means something to him or her, for their password. There are employees from Microsoft and Raytheon and Gartner and all of the big companies up there, and they’re bad passwords. And STRATFOR did nothing to encourage people to use good passwords. You know, so for example, you could use the password “stratfor”. You could have a single-character password. People just chose really horrible passwords, and what’s bad about this is, if you’ve got a really horrible password, and you’re using it with your .gov or your .mil e-mail address, there’s a possibility, I would hope a slim possibility but a possibility nonetheless, that that password is the password to that e-mail account as well, and you might be able to leverage that into a further break-in. It’s really important that when you’re using services like this that you make sure that the primary e-mail accounts that you use and primary credit card accounts that you use have totally different passwords. That way if something does happen to one of these services, you don’t have to worry about it impacting you. And the last thing I want to say about STRATFOR is, you know, obviously there’s a lot of people talking about this. A quick search of the web will bring up hundreds of thousands of hits for STRATFOR right now. But somebody did take a little time to put together website security lessons, and I thought this was an interesting article, and maybe people out there could use it for, if you’re running your own website, here’s
some things that you can do that, you know, sort of “lessons learned from STRATFOR”. So I’ll put that up. I’ll put links to all these other articles up as well.

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