Hello, I’m Roger Safian. Today is Thursday, September 29, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

We got a story this week about how Windows machines get infected with malware. And basically, this is a statistical analysis of some large number of infected hosts and how they connected to the network. Primarily I believe this is through the browser is how they were determining this stuff. But basically what they’re saying here, kind of interesting, 95 percent, if you look at the information that they’re putting out, 95 percent of these infected machines would have avoided their problems if they had an up-to-date browser, if Java, Flash, and Reader were up to date. Just those four things. If you took care of those four things, 95 percent of the time you wouldn’t be an issue. Now my suspicion is, and I’m sure you would agree, there’s more to it than just that, but it is important to keep your machine up to date, and I think the information here certainly bears that out.

Then we’ve got an interesting twist on spreading malware, and this is probably going to be most effective in a work environment. And basically, if you’ve got one of those big modern copy machines now, you can have that scan stuff and then send it to you, typically as a PDF, send you the attachment or maybe you want to set it up so that it’ll do faxing or something like that. But what the malware is doing now is sending e-mail messages with a malicious attachment that potentially looks like something that might come from your copier. And, you know, that’s kind of a clever little twist I would say, so keep your eye open. What I would say is, look, don’t not use your copier to do this stuff; I mean, obviously people need to be able to do things. But if you’re not expecting something from the copier, and the copier sends you something, be a little cautious before you open it. The copier is probably not trying to be your buddy or anything like that, it’s unlikely to just send you something out of the blue. Doesn’t mean that somebody else couldn’t have sent it to you as part of a CC or something like that, but just sort of keep it in mind. If you’re not expecting something from the copier, or for that matter from anybody else, with an attachment, just be a little cautious when you actually open those things up. And remember, keep your antiviral software up to date so that you’ve got the best chance of catching this stuff.

Then, there was an article I read about Bluetooth security issues. Basically, what they’re saying is, Bluetooth is not necessarily that secure. The concern here is that, as Bluetooth becomes more and more prevalent, you know, it’s in cars, it’s in health care equipment, it’s, you know, a
lot of different places where Bluetooth is, it’s not just on your computer. But, I don’t know, I
guess I’m just not going to get wrapped around the axle about insecure Bluetooth in my car.
What’s the real risk that somebody in the vicinity where I’m driving is also driving in the same
direction as I am and is going to be able to pair up with my car and then make some sort of
phone call using my car Bluetooth, but that’s really their connection? I mean, the whole thing
seems kind of ridiculous. What I would say, though, is where Bluetooth issues are probably
more concerning is if you’ve got a device like your computer, maybe even a smartphone, if
you’ve got Bluetooth there, now you’re probably stationary and somebody could do it, and
maybe get more information than they could just from my car. What I would say, though, is if
you’re not using Bluetooth, just turn it off. It might be on your computer, it might be on your
smartphone, just turn it off. And as for the health care thing, absolutely, they should be making sure that these devices, especially devices that
they put a device in that’s monitoring your heart or your diabetes or something like that, you
want to make sure that stuff is secure. On the other hand, there has to be a balance here.
Doctors are not information security professionals, but definitely I think you want to make sure
that, especially where somebody’s life is at risk, that you take some extra steps there.

And then I wanted to follow up: dirty tricks that social engineers use. And basically what this is,
is it’s the very same thing that we’ve been talking about for a long time. It’s, you know, “donate
to the hurricane relief efforts”, or “about your job application”, but it’s kind of an interesting
read about things that the social engineers do trying to get people to click on links, trying to get
people to click on malicious malr a while, I think we’ve been talking about this stuff a lot, but it
still happens, and ware, clearly these people are bad. It’s an interesting article. When you see
all this stuff together, it looks to me it’s kind of striking. These are obviously techniques that are
successful. If they weren’t successful, my guess is they probably wouldn’t use them.

Then the last bit about malware that I want to talk about is malware that spreads as a browser
update. We’ve seen some of this stuff here on campus, fortunately, not a tremendous amount,
but basically what happens is a user gets a message on their screen that says, “Hey, there’s a
new version, a browser update is available”. And, you know, everybody’s trying to encourage
users to update their stuff all the time, so when they see this, they just naturally click
on it. And
it’s not a message from the browser telling you that it’s an update, it’s malware that’s going to
install itself on your machine. When we’ve seen this, it’s been TDSS, and what else it does
afterwards then is the machine that’s infected starts acting as a DHCP server on the local
network, so you’ll start seeing lots of machines get these browser update messages on your
local network. What you can do, if you do get this infection, is check your information for DHCP
server, and then that’ll tell you where the infected machine is, and then you can go deal with
that infected host hopefully before it becomes more of a problem.
And then I want to close with a Facebook scam. Basically, a woman got heisted out of two thousand dollars because she thought it was her sister she was chatting with in Facebook, and the Facebook scammer told her, “Hey, I just signed up for something and I got access to a half a million dollars for two thousand dollars”. I mean, I would say two things here. One, you’re not going to get a half a million dollars for two thousand dollars even from your sister. And if it’s your sister and you think she’s telling you the truth and stuff like this, don’t just handle it over chat in Facebook; call your sister up and talk to her. You know, there’s a lot of people out there that get messages, whether it’s “I’m trapped and I don’t have my credit cards in London” or something like this, and people just automatically send off information or money to these scammers. Don’t do this stuff! If you think there might be something legitimate here, follow up with it. Call the person. In this particular case, it would have been trivial for this woman to just call her sister and talk to her instead of just relying on the scammer that had hacked her sister’s Facebook account.

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