



THE MALWARE REPORT

Hotel Business Center PCs Strike Again

Participants:

Matt Grant, host

Randy Abrams, director of technical education, ESET, LLC

The Malware Report Transcript

Title: Hotel Business Center PCs Strike Again

Episode: 135

Location: http://www.eset.com/podcasts/073009_ESET_Business_Center.mp3

August 20, 2009

[Begin recorded material]

Matt Grant: Hi, this is Matt Grant, and you're listening to The Malware Report with Randy Abrams. Hi, Randy, thanks for being here.

Randy Abrams: Hey Matt, it's great to be back.

Matt Grant: You know, I wanted to chat about a topic that I know we've discussed on the show before and that is hotel business center computers and some of the documents that unfortunately get left behind as folks check out of these hotels. I know you took a trip recently back to South Carolina and found some interesting things on the business center PCs there. Do you want to tell us a little bit more about that?

Randy Abrams: Sure, I actually found a variety of interesting information. Some of it was related to businesses and some of it was related to people, it was personal. On the personal side, I found a temporary Internet file that

had a complete Yahoo! email, so it had the “From” address and it had the “To” address and in this case, it was a purchase confirmation. A woman had bought some things at an online store and so I knew what she bought, I knew when she bought it, I had her UPS tracking delivery number in the copy of the email that was left on the computer, her name, phone number, where she lives at; all this information. You know, it might not sound like much, except that for an attacker, that’s enough information to very effectively socially engineer a user. So, I found a letter titled “A letter to just one of the other women” and fortunately the author didn’t include last names. However, what she didn’t realize is that Microsoft Word and Office stores the registered owner’s name in the document properties and so potentially that’s a way to identify a unique individual, but the letter actually had some fairly racy stuff in it like, “Are you the woman that our 3-year old saw in our quote, unquote ‘Mommy’s bed in the bed and the bed was rocking?’” You know, things like that that probably weren’t meant to be seen by other people.

Matt Grant: Are these people taking any lengths to delete these files once they use the business center computer or are these files not even deleted from the machine?

Randy Abrams: In the case of the email purchase confirmation, the person probably didn’t know that Internet Explorer was saving temporary files. It’s common for browsers to save temporary files and so it’s a really good idea if you’re using a business center computer, that you delete the temporary Internet files as soon as you’re done to avoid this kind of compromise. In the case of the letter to the other woman, I think the person just forgot to delete the document after she finished writing it because the document wasn’t a temporary file; it was just there left behind. But it’s not just home like users that do this kind of thing. There was a letter I found that had to do with a site visit to Charleston

Air Force Base and fortunately, there wasn't any classified information in this document, but still, by policy the military probably should make sure that both active-duty and civilians working for the military know not to talk about military stuff on public computers and it's not just hotel business centers, but any public computer. I also found orders for someone being assigned chief officer of a commercial vessel. He probably saved that document because he needed to print it out—it said "You need this paper to get on board the vessel."

Matt Grant: Right, interesting. What type of procedures should people use when they are using these type of public or hotel business center computers to try to protect their information that they may be using that computer for?

Randy Abrams: Quite frankly, there's very little that these computers are safe to use. One of the things I found on this computer was that it had been infected by at least five pieces of malware previously that their antivirus had cleaned up, but the computer had been infected. When you use a public computer, you don't know if there's a keystroke logger on it. So, you have to go in and assume everything that you see on that computer is public information. That means if you read an email, you see it, so it's public information. Everything that you type on that computer is public information. If you type your password to your Yahoo! email account, assume its public information. If you VPN into your corporate network, assume someone else has your credentials now and can get onto your computer, onto your corporate network account. There's just no safe way to use these computers. So, there's basically three things that I will use a business computer center for. One, if I have a confirmation number, I'll print out my flight confirmation; I don't care if someone knows that I'm on that airplane if they're already in the same city. The second thing is if I want to just do some non-specific web research, I want to see "What's the price of

my stock today?" I don't care if someone else knows that's the price of that specific stock, that I look it up they don't even know I own it and that doesn't matter to me. The third thing is to find out the interesting things people leave behind on hotel business center computers.

Matt Grant: You know, this was a rather large hotel chain here in the U.S. Are they going to any lengths to have any sort of security on these computers or not?

Randy Abrams: Well, that's interesting because although it's a large hotel chain, many of the individual hotels are franchised. So, I've been to some of these hotels where the computers are really locked down. In fact, essentially the computer is what we call a kiosk and you can't do a lot with it. Other computers I've gone to at this hotel chain, I've been able to get pretty far without doing any real hacking, if you will, just using what's available by clicking on folders and looking at files, things like that. So, it really varies. In my experience, hotels are getting a lot better at managing their business center computers. I used to stay at another one of this chain's high-scale properties in Dublin, Ireland and every time I would go there, I would get a free pint of Guinness from the bartender for disinfecting their business center computer. Last time I was there, they had it locked down really, really well.

Matt Grant: So, what should they be doing? What are some of those things they should have in place?

Randy Abrams: Well, I think number one, they ought to have a big sign up saying, "Remember, anything that you can read or see on this computer, someone else probably can too." Participate in education, let people know that these are not the kinds of computers that you use to conduct business or share highly personal information on. It's a really good idea to lock these things down; there's a variety of software packages available that put the computer kiosk into kiosk mode, if you will. This hotel that I was at was using Vista and it had limited user accounts. So,

I wasn't an admin on this computer, I was a very limited user and still found all this information

Matt Grant:

Well that's interesting, Randy. I appreciate you taking the time to talk to us today about this and how we as the user can keep ourselves safe and also what the hotels should be doing to help keep their guests safe on the business center as well. This has been Matt Grant and you're listening to the Malware report with Randy Abrams. If you have any additional questions for Randy, feel free to e-mail him at askeset@eset.com and you can follow the ESET research team on Twitter @esetresearch.

[End of recorded material]