



## **THE MALWARE REPORT**

### ***Radisson Hotels Exposed by Guest Data Breach***

#### **Participants:**

Matt Grant, host

Randy Abrams, director of technical education, ESET, LLC

#### **The Malware Report Transcript**

Title: Radisson Hotels Exposed by Guest Data Breach

Episode: 140

Location: [http://www.eset.com/podcasts/090809\\_ESET\\_Radisson.mp3](http://www.eset.com/podcasts/090809_ESET_Radisson.mp3)

September 23, 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 joining us.

Randy Abrams: Well, thank you for having me back again.

Matt Grant: You know, I wanted to chat about a topic that the Federal law enforcement is actually investigating and that is a hack that compromised computer systems at Radisson hotels and resorts throughout the U.S. and Canada. Can you tell us a little bit more about this breach?

Randy Abrams: Well, from the information that I've seen, what happened was someone hacked into some of the Radisson hotel computer systems and it was I believe about 400 hotels that were affected. But, the data that the hackers may have accessed could include the name of the

guest that's printed on the credit card or debit card, the actual credit card or debit card number and the expiration date. If that's the limit of the information they got, it's not too damaging. Getting that little three-digit code or four-digit code on the back of the card makes things a bit easier for the bad guys, but there are lots of ways that the bad guys get information and can cross reference it. So, this is kind of a bit of a black eye for the Radisson; it's happened to other hotels as well, but it's not like a business-shaking event. However, I travel a lot, I stay at a lot of hotels throughout the world and honestly, in general, hotel security around guest data is pretty dismal. I mean, I've been at hotels where they slide your bill under the door on your last night, but they don't slide it all the way under the door. So, anyone walking down the hall can pull it out and open it and can get a fair amount of information about you. One hotel I was at and it's a pretty big name hotel chain, my bill was left actually outside the door as were all the other guest's bills. If I'd been interested, I could have gotten a fair amount of information about these other guests as well. And when you go to the hotel business center computers, a lot of people don't understand that a lot of data can be left behind. So, I've come across in my research, hotel reservations from Yahoo! email accounts to the same hotel chain in a different city. So, it definitely hurts to have the information compromised as Radisson had in this case because you got credit card numbers, but it really compounds the issue when they make it so easy. And I'm not picking on Radisson for this, hotels in general make it so easy for bad guys to also get other information if they're physically on the premises.

Matt Grant:

Right. Do you know, I guess how the bad guys hacked in in this case and what should both Radisson and other hotel chains be doing to protect those computers?

Randy Abrams: Yeah, I don't know in this case, I didn't see any information on how the hackers got in and I suspect they're not releasing it because it's an ongoing investigation. But, it's not just Radisson and other hotels, but businesses in general need to do things like hire penetration testers to ensure the integrity of their security, make sure that they've got really robust security. Employee training is huge; it's quite possible that the computers in this case were compromised because an employee got phished. So, teaching employees how to avoid phishing attacks to understand that Help Desk doesn't tell them to change their password to something that Help Desk knows. You know, Help Desk doesn't say, "Change your password to 1\*259." I mean, it could look like a great password, but Help Desk doesn't tell you what to set your password. If Help Desk calls you on the phone and you don't actually know that person; don't know his voice and all that; can't look him up in the global address book and call him back; don't believe it because that's another common social engineering attack that's been around since Kevin Mitnick was hacking before computers really. So, there's some standard security computer practices that are very overlooked and organizations that want to protect the integrity of their customer's data need to look into this and do it right.

Matt Grant: Absolutely and I think the responsibility definitely lies on the business to keep customer information protected, but what can, if anything, the customer do in this case? The hotel guest, how does this affect and what could they do after the fact and what could they do in the future when staying at a hotel in case something like this happened?

Randy Abrams: In this case, the Radisson sent a letter to guests that had stayed during the period they knew they were vulnerable and offered a year of free credit monitoring/free credit reporting and guests should take them up on that. There's really nothing the guests can do other than monitor their credit card bills. Every year, you can get a free credit report form

the three biggest credit reporting agencies in the U.S. anyway. So, you know, keep on top of that stuff and watch out for these things, but once you hand that data over to someone else, you entrust it to them and if they mess up, there's nothing you can really do to stop them, So, you know, take your normal precautions. You can use credit cards with low limits for certain things, you know, which is what we call segmentation. Actually it applies to networks, but it applies to lots of things in life as well. So, you can use specific credit cards for specific things and maintain limits that are only as big as you need, but in the end you just have to live life and understand that each time you get in your car go to a movie, you put your life at risk because of a car accident. So, do what you can to do it right. Mitigate risks, but don't live your life being afraid of everything.

Matt Grant:

Good point and definitely a fair one. So, thanks so much, Randy for taking the time to explain a little bit more to explain this breach in detail and what folks can do to stay protected and what businesses should be doing as well. If you have a question for Randy, feel free to e-mail him at [askeset@eset.com](mailto:askeset@eset.com). You can also follow him on Twitter @esetresearch. This has been Matt Grant and you're listening to the Malware report with Randy Abrams.

[End of recorded material]