



THE MALWARE REPORT

2009 Black Hat Conference Highlights

Participants:

Matt Grant, host

Randy Abrams, director of technical education, ESET, LLC

The Malware Report Transcript

Title: 2009 Black Hat Conference Highlights

Episode: 133

Location: http://www.eset.com/podcasts/073009_ESET_Black_Hat_09.mp3

August 6, 2009

[Begin recorded material]

Matt Grant: Hi, this is Matt Grant, and you're listening to The Malware Report with Randy Abrams. Hi, Randy, how are you?

Randy Abrams: Great, thanks. How are you today?

Matt Grant: Pretty good, thanks so much for joining us today. I know you've been following the Black Hat Conference in Las Vegas that took place last week. Why don't you tell us a little bit about what Black Hat is for some of our listeners who might not know and then maybe we can talk a little bit about what's coming out of the show.

Randy Abrams: Fundamentally, Black Hat is an excuse for security experts to get together, drink beer and brag about what they found.

Matt Grant: Sounds like fun.

Randy Abrams: Oh yeah, it's definitely a blast. Unfortunately, I didn't get to go there this year, but a lot of my friends are there and there've been some

interesting stories out of it. One of them had to do with a couple of hackers, one White Hat, one Black Hat, that have had their accounts hacked. Dan Kaminsky is one of them. Last year, he did a highly publicized presentation about some serious flaws in DNS and the other hacker was Kevin Mitnick. And interestingly, the people who hacked their accounts and released information claim it was because these people are all about hype and they don't do anything to help secure people. And, of course, the hackers were suffering from a severe case of cyber weenie envy; they did nothing to help security, they just wanted attention themselves. But you know, even skilled professionals can get hacked; there's a lot of stuff to take care of. In Dan Kaminsky's case, he wasn't actually using really good passwords either. There's also an interesting story about the smart meter which is coming to your home if it isn't already there, and that's your electrical...

Matt Grant: I think we talked about that topic a few weeks ago on the podcast. Maybe you can just give a quick overview, what exactly is a smart meter again?

Randy Abrams: It's your electrical meter. They come out and read how much energy you've used. But the new smart meters, instead of them having to come out and read it, they'll be hooked up to your home via the Internet and so that means that there's the potential for abuse. And in fact, it turns out that the company who's making the smart meters was far more interested in functionality than security. And so, a couple of researchers talked about ways to attack the smart meters and actually run a worm; a self-replicating program that can copy itself from one smart meter to the next in a neighborhood and potentially that could cause power outages; potentially someone could steal electricity; potentially it could be a way back in to hack the power company's systems as well.

Matt Grant: You would think with this information available now on some of the vulnerabilities with the smart meter that they would try to beef up the security before actually implementing these in homes. Is that the case or is it looking like they're gonna be implementing these as is and we'll probably be looking at some issues in the future?

Randy Abrams: Oh it's too late; these meters have actually already been implemented. So, what they're going to have to do is go back now and fix the problems and try to make them much more secure. And I honestly don't know if that means they're going to actually have to swap out some of the old insecure ones for newer ones with better security because it was obviously not designed to begin with for security and sometimes when that happens, you just have to use different components to make things secure.

Matt Grant: Absolutely. What do they need to be doing to make things a little bit more secure?

Randy Abrams: Well, for one thing, the meters should not be able to run any software that isn't digitally signed. So, you should have to have a digital signature on it and that's one of the big things. There's just a whole slew of things they need to do. They really need to use extensive defense in depth. So, you shouldn't be able to get into that system and if you can access that computer system, there should be multi-level authentication required. So, even an authorized technician coming to your home to work on it should have things like a password as well as a hardware device before they're allowed to make any changes, much less read the data from these meters. It's mind boggling how little security obviously went into it if you can put in an unsigned program such as a worm and run it on multiple meters. It's just mind boggling.

Matt Grant: Interesting. Any other topics or news coming out of the show that's been of interest to you?

Randy Abrams: Yeah, one of them actually has to do with digital certificate technology. Digital certificates are designed to let you know that the program that you're going to run hasn't been tampered with. Some people think that it's antivirus—it's not antivirus—but there's a demonstration and Dan Kaminsky again illustrated this, they call it flaws in X.509 authentication—which X.509 is a standard. And according to Kaminsky and another researcher as well, Moxie Marlinspike, demonstrated attacks that spoof SSL certificates, which are a type of certificate that's used for other things. You know, there are some problems where you can actually attack these digital certificates so they lie to you. They don't actually prove the software is what it is supposed to be or the website is what it's supposed to be. So, it just goes to show that right now, we're really in the early ages of computer security. And computers haven't been around that long in terms of technologies that are in our lives. You can expect that in 10 to 20 years, the landscape is going to be quite different because security is now getting focused and has been for a short time now, but where we're at today—it's pretty primitive.

Matt Grant: Very interesting. Yeah, absolutely and very insightful. It will be interesting to see what continues to come out of future Black Hats and thanks so much for taking the time to give us a quick snapshot of what's coming out of this year's Black Hat conference. If you have any questions you would like to ask Randy, feel free to e-mail him at askeset@eset.com and you can follow the ESET research team on Twitter @esetresearch. This has been Matt Grant and you're listening to the Malware report with Randy Abrams.

[End of recorded material]