



THE MALWARE REPORT

Employment Scams: Taking Advantage of Desperate Job Seekers

Participants:

Matt Grant, host

Randy Abrams, director of technical education, ESET LLC

The Malware Report Transcript

Title: Employment Scams: Taking Advantage of Desperate Job Seekers

Episode: 117

Location: http://www.eset.com/podcasts/032409_ESET_Employment_Scam.mp3

April 16, 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: Hi, Matt. It's great to be back.

Matt Grant: I wanted to spend some time today talking about something that seems to be increasing these days with the current economy and that is attacks or scams targeted at job seekers. Have you seen this or an increase in this particular type of attack?

Randy Abrams: This really encompasses a broad range of security issues. There's a Web site, www.privacyrights.org that actually talks about avoiding online job scams. One of the things they talk about is job seekers who use an online job search Web site, they need to be careful to avoid a type of job scam where you apply for a job and then you're asked to accept payments into your own bank account. You hope most people

would realize there's a problem there. But this is how the money mules are recruited and with people being out of work and unemployment being high in some areas, people are getting a bit desperate for jobs. The criminals will make it sound like they're offering you a legitimate job - they'll call it accounting or payment processing and they're going to use your bank account to deposit stolen money into and you get to keep a percentage of that money and send them the rest of the money. What happens then is the bank catches on that it was stolen money and the victim (the job applicant) is on the line for all of it - the money they got to keep, as well as the money they sent back to the criminal organization.

Matt Grant: Interesting. How are they getting the information of these job seekers? Is it through email, phishing scams, or is it through targeting sites like Monster.com or CareerBuilder?

Randy Abrams: You know, there are some different approaches. One of them is just blanket spamming. When you've got a fairly high unemployment rate, spam is really cheap, you can spam randomly. Another problem is when a Web site like Monster.com gets compromised - which has happened before - and the bad guys get a database containing the names and at least contact information if not more, for the job applicants. Then you get the targeted attacks where the attacker knows someone is looking for a job. Depending on the information that was compromised, they might even know what that person's skill set is. And so they can direct phishing attacks that might not even be a job offer, but just might take advantage of having enough knowledge to successfully perform fraud or they might offer a job that isn't a legal job.

Matt Grant: Interesting. Do you think with the current desperation in employment, folks are more likely to fall for these scams now than in the past? Or

do you think it's just ratios that because there are more folks who are unemployed then there are going to be more people who fall for them.

Randy Abrams: I think it's a combination because when you've got more people who are unemployed then you've got more of the people that would have the propensity to fall for them. There is probably some desperation aspect where "Okay I'm not finding the kind of job I want, I need a job, this is a job I'm going to do for a short time until I can find what I want."

Matt Grant: Yea, absolutely. Is there something they can look for in these particular types of attacks?

Randy Abrams: If you're asked for a bank account number before you actually get a job, PayPal account number or credit card number, that's a really bad sign. In general, the only reason to give a bank account number is if you've got a job where they're going to direct deposit your paycheck - not someone else's money - but your paycheck. There's no reason to give your employer a PayPal account that I can see or a credit card number either. So, you don't want to agree to have your funds direct deposited by a new employer you've never met. Now, on the Privacy Rights Clearinghouse Web site, they say do not agree to have funds or paychecks direct deposited to any of your accounts by a new employer. Well you've got to use some discretion there. It's like when I joined ESET. I knew the company ESET, I knew who I was dealing with - yeah, you can direct deposit my paycheck that's fine. But if I got a job with some company and I've never even met any of the people at it, no, I'm not going to give them my bank account number.

Matt Grant: Absolutely. In addition to some of the discretion is there anything else that job seekers can do to avoid these scams or in the type of applications they are submitting or ways they're going about looking for employment?

Randy Abrams: It's always a great idea to do a little searching and research on the company that you're going to potentially work for. One of the things I would recommend is to type in the name of the company and the words "fraud," "scam" or "complaint" and see what Google or your favorite search engine turn up. Just that little step can oftentimes reveal that this isn't someone you want to deal with.

Matt Grant: Interesting. Well Randy, this is extremely helpful information - especially as folks are I'm sure looking for jobs in this tough economy. It's important to remember some of these tips to protect yourself and your identity. If you have any questions for Randy on this topic, please feel free to e-mail Randy at askeset@eset.com. This has been Matt Grant and you've been listening to the Malware report.

[End of recorded material]