



THE MALWARE REPORT

Twitter Links Lead to Trouble for Blind Followers

Participants:

Matt Grant, host

Randy Abrams, director of technical education, ESET LLC

The Malware Report Transcript

Title: Twitter Links Lead to Trouble for Blind Followers

Episode: 116

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

April 9, 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 our show again.

Randy Abrams: Hi, Matt. It's great to be back again.

Matt Grant: So, I wanted to spend some time today discussing a topic that was recently written about and that was that researchers at Secure Science have devised a new Twitter attack they say could spread virally like a worm through Twitter. Have you heard of this?

Randy Abrams: Yes, I have. I actually saw the article about that. It might be negligent not to point out that Twitter isn't the only social networking site that can be vulnerable to these types of attacks. One of the enablers was a cross-site scripting flaw and those vulnerabilities have been cropping up all over the Internet, not just with social networking sites. However,

with social networking sites, it becomes a lot easier to propagate things. I'm not exactly sure if worm is the exact word, but because people tend to have many contacts and these attacks can automatically send an unauthorized message to all of a person's contacts and the people receiving them believe their friend actually sent the message, they're likely to click the links.

Matt Grant: Interesting. They were mentioning that the hack is similar to a click-jacking attack that was making its rounds on Twitter last month. Are you familiar with this attack and I guess why the need to attack a social networking site in particular?

Randy Abrams: I'm familiar with that attack. The answer to why the need to attack social networking sites - it's because it makes social engineering so much easier. Part of social engineering, a big part, is trying to convince someone to do something that they wouldn't want to do if they didn't know what it was. The easiest way to convince many people to click on a link, which is where the trouble generally starts, is to make the message come from a trusted source. On social networking sites, people tend to let their guard down and instantly assume that any message, no matter how out of the blue or irrelevant it seems, came from the person that they thought sent it. So people will click on the links and because of the nature of a network, it isn't just one-to-one, you compromise one account and you send messages to potentially dozens, hundreds, even thousands more accounts. That makes social networking sites a very low-cost high-yield attack vector.

Matt Grant: Interesting. Is there something in particular that Twitter needs to be doing or social networking sites need to be doing to better protect their service or is this something that really does lie with the end user's education to these type of attacks?

Randy Abrams: There's a combination of defenses here. Yes, Twitter needed to disable the cross-site scripting flaw which allowed the specific attack to

happen. Web browsers are increasingly attempting to prevent cross-site scripting. I know Microsoft's Internet Explorer 8 has some enhancements to help prevent cross-site scripting attacks; it's not going to eliminate them. Firefox has no script, but in my experience with no script - which I have been using for a while now - it takes little bit more of an educated user to use more effectively or people will give up. You have to know when to allow things or not allow things, if you just allow everything; you might as well not have it pretty much. There are some technological partial solutions, but education is going to be the big part. Being suspicious of links that are sent to you out of the blue is a top tip.

Matt Grant: Absolutely. I guess even through these social networking sites, even with Twitter being primarily a mobile platform, there's still concerns with clicking on links, is that correct?

Randy Abrams: That is correct. That's one of the reasons I like to use Sandboxie and I've talked about that in the past - Sandboxie is a web-browser. Even a skilled security researcher can at some point fall for something stupid and make a mistake. When I get messages from the community I work with, I tend to put a little more trust in them and I am more likely to click, but I do it with the added level of protection of the web links that are Sandboxed and I don't just download and run files from anyone.

Matt Grant: Do you think it's getting easier for folks to target Twitter in particular because of some of the new free text messaging plans and the low cost to work on mobile devices?

Randy Abrams: I wouldn't necessarily say that it's easier to target Twitter. Twitter is in the enviable position of growing quickly and that draws a lot of attention. Unfortunately, it makes Twitter a higher value target. It isn't so much the ease; there are probably social networking sites out there that can be attacked a lot more easily, but the return isn't as high for the attacker. It's their success that makes them a big juicy target.

Matt Grant: Interesting. We've learned some of the rules related to email scams with not clicking on links or opening attachments from unknown senders. Do the same rules apply - should we take the knowledge that we have with email and transform that for both social networking and Twitter?

Randy Abrams: Absolutely. You need to understand - a lot of people still don't - that even with email, the senders' ID can be spoofed. I can send you an email that looks like it came from Bill Gates; the ID can be spoofed. Additionally, if my computer gets infected, it can be used to send email that actually does come from my account, but I didn't type in the message, I didn't type in the link. So, it's a good idea to double check with the sender - "Did you actually mean to send me that link?" or "Talk to me a little bit more about this link, what is it?" Make sure that everything is in context when you're dealing with the person you know.

Matt Grant: Well Randy, as always, that's good advice for our listeners. If you do have questions for Randy or would like to learn more, please feel free to e-mail him at askeset@eset.com. This has been Matt Grant and you've been listening to the Malware report.

[End of recorded material]