



THE MALWARE REPORT

Twitter Attackers Find New Followers

Participants:

Matt Grant, host

Randy Abrams, director of technical education, ESET, LLC

The Malware Report Transcript

Title: Twitter Attackers Find New Followers

Episode: 125

Location: http://www.eset.com/podcasts/060309_ESET_Twitter_Follower.mp3

June 11, 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: Excellent, thank you very much. How are you today, Matt?

Matt Grant: Pretty good, thank you. Unfortunately, there was another recent attack on Twitter. I know this is a topic we've discussed in past podcasts. I wanted to spend sometime today talking about the most recent attack – quote unquote a “Best Video” in the subject and a link to a website that downloads malicious software. Do you have any more information on this particular attack you can tell us about?

Randy Abrams: There's not a lot to say other than don't trust everything you read. If you see things about best video, funny video, funny card or things like that and you don't know who sent it to you – just because someone is following you doesn't mean you know them – it's not a good idea to

click. The Achilles heel of social networking is that people are far too eager to trust anyone who approaches them. It's not going to be the last attack that we see and is not necessarily a Twitter security issue; it's a user education issue.

In this case, there were a bunch of tweets sent out that told users about a best video. When they went to the website – it looked like they were going to YouTube, which they weren't – the website delivered a PDF document that exploited vulnerability in Adobe's Readers program. People need to learn to patch. People who aren't using current patch versions probably got hit; I'm not sure which vulnerability got hit this time. We're seeing tons of attacks against old vulnerabilities that are fixed with patches. People don't understand that even programs like WinZip need to be updated because they have security issues. Twitter did what they could by temporarily suspending accounts that might have been compromised, but they can't stop users from doing things they shouldn't do.

Matt Grant: No, absolutely. Is this similar to some of the types of attacks we've seen recently with regards to Twitter? Have there been phishing attacks? I know some of them were Twitter vulnerabilities themselves, is this the tip of the iceberg when it comes to phishing attacks that are targeting Twitter?

Randy Abrams: Well, this one wasn't a phishing attack. In this case, when you went to the website to download the PDF, it exploited that and came up with a dialogue saying you need to clean your infected system and tried to sell you antivirus software that wasn't antivirus software. This is a huge for-profit venture that is different than phishing in that it's not trying to trick you into giving up account information by typing it in, but by tricking you to get you to pay for useless software and take control of your computer. I didn't look at the exact rogue program, but

the odds are that it would also install a bot and make your computer part of the Botnet.

Matt Grant: Do we know if there is one criminal group behind this?

Randy Abrams: I suspect that it's one criminal group behind this specific attack, it's hard to say. I wouldn't know for sure, but it wouldn't make sense to have more than one criminal group in an attack of this scale. I don't think one criminal group is behind all the attacks we're seeing out there. I think there are more than enough criminals to go around for all of that.

Matt Grant: Absolutely. I know we've seen similar attacks on social networks like Facebook and Myspace. Is there anything at this point where Twitter users should learn from those past attacks that have targeted social networks?

Randy Abrams: One of the best things Twitter users can learn is patience. When you get a link, give it a couple of days before clicking on it. The odds are, if it's a bad link, it'll be down, won't work and it's a good thing it didn't work because it would have infected you. If it's from someone you don't know, ignore it. But if you have to see it, give it a few days.

Matt Grant: Interesting. Good advice as always. Randy, anything else on this particular topic before we let you go?

Randy Abrams: When you get communications from quote unquote "friends," computers lie – they lie all the time. Make sure it really is that person; don't assume it's that person unless there's something significantly contextual that tells you "Yeah, this is actually my friend who is actually talking to me and this is expected communication."

Matt Grant: Thanks so much Randy. We appreciate you taking the time to talk about this topic and offer tips on how we can stay safe using these types of social networking sites. If you would like a list of sites or have additional questions, you can ask Randy at askeset@eset.com. This has been Matt Grant and you're listening to the Malware report.

[End of recorded material]