



THE MALWARE REPORT

Trojans Use Political Passions to Lure Users

Participants:

Matt Grant, host

Randy Abrams, director of technical education, ESET, LLC

The Malware Report Transcript

Title: Trojans Use Political Passions to Lure Users

Episode: 137

Location: http://www.eset.com/podcasts/082009_BTP_Spam_Obama.mp3

September 3, 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 ya?

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

Matt Grant: Good, thanks. Thanks so much for joining us today. You know, I wanted to talk about a recent spam attack that is offering to let people to use their PC to attack Obama's website. But, in reality, it seems that the spammers are hoping that Obama critics launch a cyber protest, but in actuality it looks like it downloads malware onto their PCs in the process. Can you maybe explain this to us in a little more detail?

Randy Abrams: Well, sure. It's an age old type of social engineering trick. The idea is to appeal to people's emotions and in this case to convince them to do something that's illegal anyway, which a lot of social engineering

doesn't try to get people to do things that they know are necessarily wrong or illegal. But, in this case, DDoS (distributed denial-of-service attack) is illegal and what happens is instead of these people attacking Obama, they get infected with malicious software. So, the software they are downloading doesn't do at all what it claims to do, which is the classic Trojan horse. It looks like something you want and it does something malicious and unwanted in return. So, and we've seen this in a variety of situations, not always is it a matter of infecting computers because there have been attacks both against Estonia, apparently against Georgia and against Hamas from Israel, which a really good friend of mine in Israel helped put the end on that. But, different groups said, "You know, install this software and attack our enemies." Well, in this case, instead of actually attacking the enemy, it's attacking the people who installed the software. So, you know, when you play with fire, you get burned.

Matt Grant: Yeah, absolutely. It seemed like in addition in this case, the email provided a link to a website where visitors are offered money for installing this supposed denial-of-service software. Was that probably another form of motivation for them doing this?

Randy Abrams: Right. You know one thing to say, "Okay, help us attack this website," and you'll get some fringe elements that are doing that. And then you say, "And, we'll give you money to do it" and the ones that were kind of on the line about "Well maybe I shouldn't do that, and oh I get money for that too." And then you take into account the state of the economy and current state of unemployment, and you get people that are desperate for money and their political views might be "This guy is really bad, he deserves to be attacked; I can help attack him; I can get some money and I really need the money." So, the perpetrators of this scam are pretty savvy at social engineering and they're using offense in-depth instead of defense in-depth.

- Matt Grant: Yeah, absolutely. So, I guess after this happens, what happens to the PC at that point?
- Randy Abrams: Well, at that point, the PC gets infected and it's not clear what the software does exactly, but they can download anything to that PC; it could be a bot, in which case with the bot, it automatically updates. So, data can be stolen off the PC, the PC can be used for distributed denial-of-service attacks. And let's say it was, just for the sake of argument, let's say it was some fringe Obama supporter that initiated this, they could then use those PCs to attack Republican websites. Some people would say, "Yeah, that makes sense it was some fringe Obama supporter or some Obama supporter," but it could easily have been some Republican supporter trying to make Democrats look bad; it's really impossible to tell. And the odds are that it's someone that doesn't care about politics at all, but saw, "Hey, I can get a whole bunch of people to do this." Once those PCs are infected, they can be used for click fraud which is a way for other people to make money stealing advertising money actually. They can be used to store illegal content on people's computers. So, I've got a bunch of illegal MP3s, I'm not storing them on my computer, I'm storing them on your computer and let the Recording Industry Association of America come after you instead of me. So, you know, it's not much different really in effect than any of the other malicious software attacks we see, the only difference is the novel social engineering approach of "Hey, attack this politician."
- Matt Grant: So, I mean overall should people be suspicious of these type of emails and what can they look for to make sure that they're not involved with this type of attack or scam?
- Randy Abrams: You know, frankly, as big as an advocate as I am on education, the people that would actually participate in trying to perform a distributed

denial-of-service attack are so stupid that they can't protect themselves, they just don't have the mental capacity; it's that simple.

Matt Grant: Interesting, anything at this point that they should do?

Randy Abrams: They should format their hard drives, pack up their PCs and take them back to the store that they got them at because they aren't qualified to use a computer. There's antivirus software that can get removed, but these are not people that are currently at the intellectual level where they can even learn to protect themselves because they're too interested in committing crimes.

Matt Grant: Yup, absolutely. No, good point. If you have any additional questions for Randy that you're interested in asking on this topic, feel free to e-mail him at askeset@eset.com. You can also follow Randy on Twitter @esetresearch. This has been Matt Grant and you're listening to the Malware report with Randy Abrams.

[End of recorded material]