Watching the battle between Facebook and Facebook spammers

devblogs.microsoft.com/oldnewthing/20110518-01

May 18, 2011

Raymond Chen

I am watching the continuing battle between Facebook and Facebook spammers with detached amusement. When I see a spam link posted to a friend's Facebook wall, I like to go and figure out how they got fooled. Internet Explorer's InPrivate Browsing comes in handy here, because I can switch to InPrivate mode before visiting the site, so that the site can't actually cause any harm to my Facebook account since I'm not logged in and it doesn't know how to log me in. The early versions were simply Web pages that hosted an embedded YouTube video, but they placed an invisible "Like" button over the playback controls, so that any attempt to play the video resulted in a Like being posted to your wall. Another early version of Facebook spam pages sent you to a page with an embedded YouTube video, but they also ran script that monitored your mouse position and positioned a 1×1 pixel Like button under it. That way, no matter where you clicked, you clicked on the Like button. A more recent variant is one that displayed a simple math problem and asked you to enter the answer. The excuse for this is that it is to "slow down robots", but really, that answer box is a disguised Facebook comment box. You can see the people who fell for this because their Facebook wall consists of a link to the page with the comment "7". My favorite one is a spam page that said, "In order to see the video, copy this text and paste it into your Address bar." The text was, of course, some script that injected code into the page so it could run around sending messages to all your Facebook friends. The kicker was that the script being injected was called `owned.js`. (The spam was so unsophisticated, it made you copy the text yourself! Not like this one which puts the attack string on your clipboard automatically.) I started to think, "Who could possibly fall for this?" And then I realized that the answer is "There will always be people who will fall for this." These are the people who would fall for the honor system virus.

Update: On May 20, I saw a new variant. This one puts up a fake Youtube [sic] "security" dialog that says, "To comply with our Anti-SPAM™ regulations for a safe internet experience we are required to **verify your identity**" by solving a CAPTCHA. (This makes no sense.) The words in the CAPTCHA by an *amazing coincidence* happen to be a comment somebody

might make on a hot video. Because the alleged CAPTCHA dialog is a disguised Facebook comment box. The result is that the victim posts a comment like “so awesome” to their own wall, thereby propagating the spam.

Raymond Chen

Follow