



July 20, 2007

## SPAMMERS USE PDF TO BY-PASS SPAM FILTERS

Darryl D Eggleston

More and more websites are reporting the use of PDF files being used for spam. Initially most of the spam PDF had been for the use of “pump-and-dump” schemes.

Kim Komano addressed this in her July 18, 2007 Tip of the Day. She points out, “Pump-and-dumpers buy heavily into little known companies. They pitch (pump) the stock to dimwitted people through spam. When the suckers buy the stock, its price rises. The promoters then sell (dump) the stock. The stock falls back, leaving the suckers with losses.” (See more of her tips [here](#).)

However, now spammers are switching to fake prospectus.

[TechDirt.com](#) (Mike Masnick, “Stock Spammers Now Attaching Bogus Prospectus PDF,” June 25, 2007) reports, “Stock spammers keep pushing the boundaries to get around both spam filters and people’s resistance to their pitches. For a while, they were focused on using image spam to get through text filters, but now it appears that some are trying to get around filters (both technical and human) by looking a bit more legit. A group of German pump-and-dump spammers are apparently attaching a bogus stock prospectus on the stocks they’re pumping (and dumping). The attachment is a PDF file, so it gets around most spam filters, and the document is designed to look like a normal stock report (to get around human skepticism filters). It makes you wonder, if these stock spammers are going to go through so much trouble, why not just become actual stock analysts?”

The bottom line: Do not open PDF files from those you don’t know *and* be suspicious of any PDF offering investments, even if it comes from a friend.

---

<sup>1</sup> Published for the New Users Group of the Tampa Bay PC User Group < <http://gtbpcug.org> >. Permission for reproduction in whole or in part is granted to APCUG user groups and other organizations for internal, non-profit use provided credit is given to the author along with the copyright notice.

That friend's PC may have been converted to a zombie without the owner's knowledge is just doing the bidding of the "bot herder."

"Bot" or "zombie" is the term for an infected personal computer and controlled by someone other than the owner without the owner's knowledge.

A "botnet" is a large number of hijacked PCs controlled by a hacker, called a "bot herder." Botnets are used by spammers, criminals launching distributed-denial-of-service (DDoS) attacks and malware authors looking to spread their applications.

See my *ExcelNet News*, [15 June 2007](#), for more info on bot herders. There is more related news at my *ExcelNet News* [website](#).