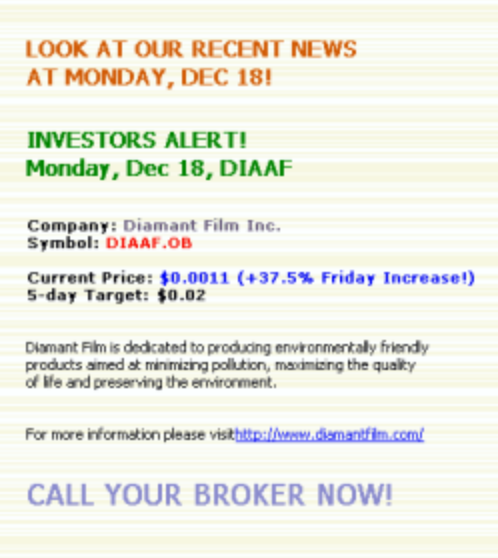
A Rustock-ing Stuffer

secureworks.com/blog/research-21041

Joe Stewart

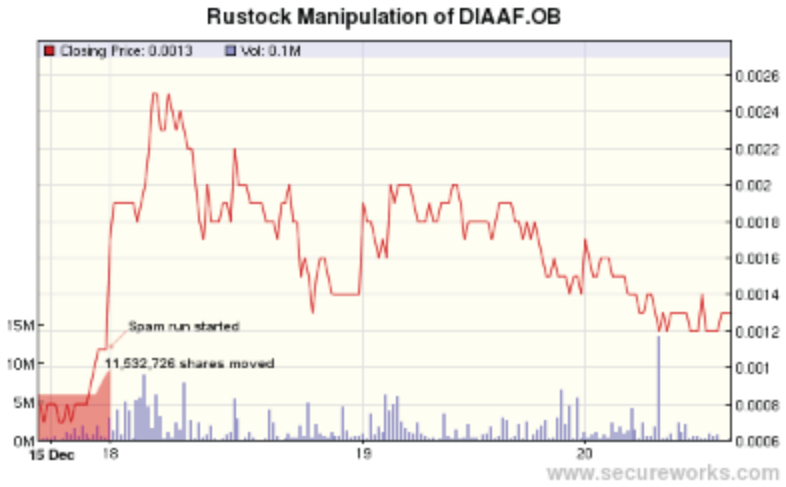
Recently I took a look at the Rustock trojan in order to see what the financial motive behind it was. No surprise, as it turns out the motive is spam. Using a sandnet, I injected myself into the botnet, able to capture (and blackhole) a small portion of the spam being sent through the system. And, as with a lot of spam these days, it's the pump-and-dump kind of spam touting penny stocks to would-be investors.



As you can see in the stock chart below, the stock was trading at $0.0008 a share when several relatively small transactions were made. In total 11,532,726 shares changed hands. Now, it's not possible to tell if these were shares bought or sold, but lets assume that these were all sold to our spammer. We can make this assumption because this stock has very little volume traded normally sometimes no shares change hands in a days time at all. So suddenly 11,532,726 shares change hands in multiple transactions in a single day, driving the price of the stock from $0.0008 to $0.0011. I'm no stock expert, but that sounds like a buy. At that price, that many shares would cost around $9,000 or so.

So, at close on Friday, December 15, the stock is at $0.0011. Suddenly, the Rustock botnet begins spewing out the spam shown above. All weekend it churns away, sending millions of emails. Monday morning, December 18, sees the stock immediately rise to $0.0019 a share, then all the way to $0.0025 a share, as some recipients of the spam begin to purchase the stock. A far cry from the spammer's target of $0.02 a share, but lets see how much that adds up to. If the spammer sells his shares early on Monday, when the stock has peaked, those 11,532,726 shares could be worth nearly $29,000, leaving the spammer with a cool $20K

profit for one weekend. I wonder if the spams touting Viagra and Rolexes have ever made that much profit so quickly for the spammers with so little effort and almost zero overhead. It's little wonder why stock spam is taking over.



I also have to wonder, are all these subsequent purchasers of the stock really unaware that this is a scam? Or are they simply greedy, hoping to cash in on the movement of the stock if they're quick enough? If you look at these stocks over time, you do see that the spamvertised stock price indeed does go up, just as the spammer predicted. If there are such day-traders who watch their email inbox eagerly for such spam, they are the engine that drives the scheme, and they are ultimately to blame for the stock spam the rest of us have to deal with.