

Hello ISSA Journal readers

What do the World Series, Hanna Montana and cybercrime have in common? Bots. In the last few weeks, a series of ticketing agencies using bots have gobbled up almost all available tickets to the games and the tween popstar's concerts and are reselling them for several times their face value. This has caused renewed interest in the software that made it possible. Bots are Internet programs used for repetitive tasks, such as comparison shopping or gaming. They can also be used to buy large amounts of concert tickets. More sinister, large collections of bots or *botnets* are also used for combing the Internet looking for email addresses for spammer's targets and spreading viruses and other malware to unsuspecting users through an open vulnerability. Many of these types of bots were introduced to the client without the owner's knowledge or permission. In large enough swarms, botnets have been used for denial of service attacks aimed towards companies and even countries.

Online retailers including Ticketmaster and Yahoo have tried to mitigate the problem by implementing safeguards to prevent or deter bots from effectively circumventing their security. One example of this is the Captcha. These are the squiggly letters and numbers that a user has to type in a box manually. However, some companies such as RMG have bot software that can circumvent these "live person" verification checks and capture this information. Ticketmaster is in the process of suing them because they claim that RMG violated their terms of use, and law enforcement agencies are leveraging existing anti-scalping laws.

The FBI has announced operation Bot Roast to try and suppress botnets and botmasters. These threats are becoming a concern to national security and personal privacy. Earlier this year, the ITC Compliance Institute reported that Symantec's biannual report counts about six million infected computers belonging to about 4,700 botnets around the world. Legislators worldwide have started paying attention as well, and we may see some draft bills in the future.

Meanwhile, the solution for most commercial companies is to exclude bot usage in acceptable use policy; ensure operating systems, IDS, firewall, anti-virus and anti-spam configurations are up to date; and monitor for symptoms of infection. Proposed mitigation tactics for event promoters include utilizing simple, random questions about the event that only a live person can answer sensibly, and lotteries where credit card holder names are pre-matched and then drawn from a pool.

Would it be prudent to outlaw the use of bot technology? What countermeasures are effective for technologies where the "bad" usages may out-weigh the good?

Let us know – Ethics@ISSA.org

About the Authors

Betty Pierce has over 23 years experience in IT. She is the Chair of the ISSA Ethics Committee, Past President of the Denver chapter of the ISSA, and Chair of the Security Advancement Foundation.

Joe Malec has over 12 years of experience in information technology. A conference speaker and published author, he has also served as president of the St. Louis ISSA chapter and is a member of the ISSA Ethics Committee.

Ethics & Privacy – September 2007

Hi Joe and Betty:

Personally I would have very serious second thoughts of joining any employer who would use either MySpace or Facebook for any kind of factual background information and take it as gospel. But... people do lie on their applications and therein lies part of the dilemma. I think it is a safe bet that most people would be terribly upset were a day care center or preschool forced to hire a pedophile so as to avoid discriminating against his past acts, but what about the children. Someone admitting to this on an application is one thing, but to have it discovered through an Internet search... I know several lawyers would be planning their next yacht purchase.

The best practice in my opinion is to push for full disclosure during the application and interview process, and should such information be found through the firm's normal hiring practice of using these types of Internet resources, this should be stated to the applicants at some point in time before hiring. The applicant then would have an opportunity to accept or deny the findings and both go on from there.

Best regards,
Keith G. Parsons, CISSP, CISM
Scarborough, Ontario, Canada