Computer News for Law Firms

No. 26 Heckman Consulting llc October 2003

Worms, Spam, & Other Slime

The recent massive infestation of the Sobig.f Worm, with the promise of many more to come, renews the issue of how to deal with Spam/Viruses/Worms etc. At the height of the infestation, I was getting over 300 Sobig messages a day (in part due to the fact that I have a public web site and subscribe to various listservs–some 97% of spam is received by people with email addresses posted on a web site). I'm sure a few genuine messages were lost in my increasingly automatic use of the delete key.

What is the best way to deal with what is at best an annoyance and at worst something that can destroy your PC and cripple the Internet? First, it is important to understand how this particular worm worked (and, because it was so massively successful, no doubt future ones will do the same).

It had two characteristics that set it off from previous worms. First, it not only broadcast to your address book, but it also scrounged your hard drive for other email addresses (for example, in downloaded temp or Web pages). Second, it spoofed the "from" address, frequently using the address of someone *else* in your address book. Thus, if someone received a copy of virus ostensibly from me, heckman@heckmanco.com, it could actually have come from someone else who had me in their address book or even in some temp Internet file that had never been cleaned out.

About This Newsletter

Heckman Consulting is a systems integration firm specializing in the legal market. John Heckman has over 20 years experience in the legal community and is featured as a "Top Tier Technologist" on www.lawcommerce.com. This newsletter is published periodically as a service to our clients and others. For back issues go to www.heckmanco.com.

Contact Heckman Consulting at:
1 Fencove Court
Old Saybrook CT 06475
Tel: (860) 395-0881
Fax: (860) 395-0386
e-mail: heckman@heckmanco.com

While this magnified the spread of the worm, the bottom line remains that the worm spread because people have ***still*** not learned never to open (or view) attachments they are not expecting. Fortunately sobig.f had an expiration date (Sept. 10) and it stopped there.

How to deal with spam and various viruses/worms is very different depending on whether you are an individual (or a small firm with a number of individual addresses that is not using Exchange) or a larger firm with a corporate e-mail system.

At present, various surveys have concluded that slightly over 50% of all email on the Internet is spam. AOL reports blocking over 80% of all its traffic. This represents a tremendous overload on corporate and other email systems. Bandwidth costs money: Spam is not free.

Spam-Proofing Your Address

It is often said that you should never try to have yourself removed from a mailing list, because that only tells the spammer that you have a valid email address. Actually, in over 80% of cases, it is *viewing* the message that confirms your address. However, this advice needs some modification. Roughly speaking, spam can be broken down into three categories: actual porn; "sex pills" that offer to grow various body parts that you may or may not have; and commercial spam - mortgages, car loans, merchandise, etc. offered by more or less legitimate merchandizers.

Since the legitimate merchandizers don't want to alienate potential customers, the chances are they *will* remove you from their lists. When I did this systematically, I found that my spam dropped by close to 50%. It does take a week or so of effort, and you have to keep at it because retailers routinely sell their lists to new spammers (Amazon.com does this all the time, for example). I also kept my "ask whether to accept cookies" turned on - why would anyone that is deleting me from their list need to set a cookie? Just say no to cookies. But it does have an effect.

Since less than 200 companies are responsible for over 90% of all spam (and making millions doing it), if you manage to get off some of their lists, you *can* reduce the amount of spam you receive.

Another simple way to spam-proof your address is to change what you give out to people to easily understandable words (e.g. heckman at heckmanco dot com) that spam harvesters cannot presently read. For this and other techniques, see Brian Livingston's excellent "Spam-Proof Your E-Mail Address" available for $9.95 from www.BriansBuzz.com/spamproof/.

Anti-Spam Programs

There is also a variety of anti-spam software on the market, which relies on combinations of four elements: white lists (accept any email from Jones); black lists (reject any email from Jones); rules (reject anything with "Viagra" in the subject line); and Bayesian filters.

White lists are necessary (although in the case of Sobig.f, you will still get virus mailings supposedly from people on the "white list"). Black lists and rules require a lot of maintenance and in my opinion are a losing battle since spammers keep changing their addresses and subject lines, and vary spellings so that rules are ineffective (how many variations on "Viagra" have you seen?). Therefore the key to an effective anti-spam program is Bayesian filters.

A Bayesian filter does a statistical analysis of allowed and rejected email and assigns it a percentage category (60% likelihood it is junk). It continues to learn as you have more and more email. This is by far the most effective and elegant way to combat spam.

There are a number of programs that have good reputations. The one I use for Outlook is "junk-out" (See www.junk-out.com or www.wopr.com). Others include Ella (www.openfieldsoftware.com), Mailwasher (www.mailwasher.net) and SpamAssassin (perhaps the best known, at www.spamassassin.com). Junk-Out moves

(Continued over)

Worms & Spam *(Cont.)*

suspected spam to a folder called "Junk" where you can inspect and delete it. This usually takes me less than a minute twice a day. All you have to do is to look for mail from people you know or email you are expecting. As you continue to use the system, it "learns" that e.g., airline reservation confirmations are not spam.

Other approaches include "challenge-response." The first time you get an email from someone, a reply is sent to them asking for confirmation. Only when you get the response does your system let the email through. This tactic has serious drawbacks, for example, wreaking havoc with listservs and a variety of email that you may actually want (such as airline reservations or other confirmation messages).

Corporate Issues

The basic problem with all approaches is "false negatives," i.e., mail you actually want that is rejected as spam. For example a lot of spam has "Hi" or "Hey" in the subject line. If you have a rule rejecting such email, then mail from actual friends that start "Hi" will also be rejected. This is a particular problem with many corporate email filters: they are locked down so tight that wanted email does not get through. For example, a client of mine recently made an on-line airline reservation, but the corporate spam filter blocked the confirmation since it was from an "unknown" source. Similarly, entrusting your spam blocking to an ISP generally does not allow for customization that takes your particular practice or requirements into effect. ISP filters are generally more broad-based and you will get a higher percentage of false negatives, i.e., email that you don't receive that you would have wanted to receive.

In addition, corporate filters tend to require qualitatively more management to be effective, thus increasing staffing requirements. Major corporate systems for Outlook are made by Norton and McAfee. GWAVA (www.gwava.com) is an excellent system for GroupWise.

Tolerance and Trade-Offs

This problem also exists in a symmetrical form in terms of "porn-blockers" which may be installed by parents or libraries. A recently study by the Kaiser Family Foundation showed that racheting up blocking software to increase the "undesirable" sites blocked from 87% to about 91% dramatically increases the number of sexual-health sites that are blocked from 9% to close to 50%, including the simply ridiculous (recipes for preparing chicken breasts). So even aside from broader censorship issues, these blockers just don't work in a reasonable fashion.

You have to decide where your tolerance level for spam falls. If you have to let in 10 extra spam messages in order to avoid falsely blocking one desired email, is it worth it? 100 extra messages? 1,000 extra messages? The minimal extra time taken to review (even briefly) subject lines will eliminate false negatives (for example, I almost routinely deleted a message from my brother about "Isabelle" - the hurricane - because it seemed like it might be porn).

Finally, the success of recent viruses and worms only reinforces the need to observe basic anti-virus guidelines:

1. Have anti-virus software and keep it up to date.

2. Keep your file extensions turned on and never open anything with executable type extensions such as *.exe, *.com, or *.vbs.

3. Never open an email you are not expecting even if it "seems" to come from someone you know

4. Turn the preview pane OFF in Outlook Leaving it on automatically "opens" the email into the preview pane, frequently confirming your email address to spammers, and violating rule 3). ■

Heckman Consulting

Heckman Consulting will help you install, configure, upgrade and troubleshoot leading legal software programs, including

- **Amicus Attorney** and **Time Matters** Practice Management programs (makes the content of your physical files available electronically)
- **Billing Matters** and **PC Law** for Time and Billing and Accounting
- **Worldox** Document Management.

If you are currently using an older version of Timeslips (9 or 10) and are thinking of upgrading since these versions are or soon will no longer be supported, you should seriously consider Billing Matters or PC Law.

Ask for a free consultation: (860) 395-0881 or heckman@heckmanco.com ■

Heckman Consulting llc
1 Fencove Court
Old Saybrook, CT 06475

Stamp