Spam/Manly Man/Dynamic Zombie BotNets/Security Tips

So how is your sexual prowess, you manly man? Still need enhancement? Did you ever stop to wonder who referred you to the enhancement company? How about your stock picking acumen with penny stocks? Your ability to buy cheap drugs over the internet? Did you finally correct that faulty credit card information with your bank? Or help the poor Nigerian ruler transfer his millions into your bank account? Speaking of which, how is that friend or colleague who sent you that e-card? Did you open it? If you are clueless about what I just asked, then you must be living in the same parallel universe as my wife, who still manages to avoid using email. But that is another story.

For those of us who are tied to the computer, spam is ever present. In 2006, 12.4 billion spams were sent daily, and traffic is up 63% in 2007. It is estimated that spam comprises from 60-80% of all emails sent. Because roughly 8% of idiot recipients purchase from a spam, the beast continues to grow, along with billion dollar losses to businesses from loss of productivity and system slow downs. Not to mention the cost to identify and quarantine. (Note to idiot judges who purchased from spam – Jim Summers is one of the pseudonyms that Bill Haltom writes under….)

In our office, spam has increased dramatically since June. Even with multiple spam filters, we have had difficulty in controlling the new spam. The majority are in the form of emails with pdf attachments. It appears that just as the spam filters learned how to identify emails with spam graphical images incorporated into the body of the email, our low rent spam community has figured out that business has an affinity for attachments sent as pdf (portable document files.)

As you all know, Adobe created this wonderful software that allows any file to be "photographed" so that it can be electronically transferred, and read, without the need for the recipient to have the software in which the document was created. More importantly, depending upon the settings, the pdf file can be transferred so that it is not subject to modification. Also, when pdf files are sent, metadata issues are no longer a concern. Remember that Word and WordPerfect maintain a nice paper trail as to all changes and modifications in a document, and this paper trail remains with the document forever unless it is removed. And while there are ethical considerations that should prevent lawyers from trying to sneak a metadata peek at confidential information that obviously was not intended to be disclosed by the sending lawyer, business does not have that problem, and is free to look and see what someone said in a document before it was deleted or modified. So pdf files have become the transfer medium of choice for many companies who wish to avoid sending information that might be harmful.

Problem is, that mindset has opened up a whole new world for spammers, and worse, malware distributors (fancy phrase for virus sending scumbag hackers). Most businesses allow email with a pdf file attachment through the server as it was long thought that pdf files were immune from viruses. Same with Excel and Zip files. Turns out that is not the case.

According to a recent White Paper from GFI (www.gfi.com), within the last couple of years, spammers and virus makers have created an unholy alliance, in which virus hackers began renting Dynamic Zombie Botnets to spammers to obtain lists and other information from host computers infected by the little vermin. What, you ask, is a DZB? Well, that is a network of compromised computers which can be controlled by a single master. The nodes, or zombies, can run into the millions, as each little Trojan horse program inside a host computer has access to address lists and other information to allow it to expand exponentially. Have you ever received a message from someone that you you know, but did not write, advising that your email was being returned? Guess what, your computer was part of the zombie network, which probably sent a spam to everyone in your address list. It may or may not have your return address. This is how hackers are able to launch DOS (denial of service) attacks where a website is overloaded and frequently shut down when millions of computers try to access the site simultaneously. Criminals use the little zombie botnets to steal credit card information, or to scam pay per click advertising companies. Recently, the hackers realized that spam was a convenient way to deliver a virus without forcing the user to download from an infected site. And, if it was concealed inside of an innocuous attachment, it would escape detection from spam and virus filters.

So what? We have had viruses for years. Well, it turns out that pdf files with viruses can only infect the computer if the pdf file is opened by Adobe Acrobat. Lucky lawyers. Recall that Adobe Acrobat happens to be the primary program that most of us use to create pdf files for efiling with federal court. Imagine that. While much of the rest of the world opens files with Adobe Reader, which is the freebie you download and can't open a virus, lawyers or staff with Adobe Acrobat on their computers are now subject to being infected by a pdf document. Worse, we all are subject to unleashing a virus by opening a strange Excel or Zip file, based upon the same hacker architecture.

Fortunately, the major anti-virus software makers have developed the ability, with help from Adobe, to analyze the contents of a pdf or Excel file. Unfortunately, many of us have not taken the time to update our anti-spam or virus files, or to run the detection programs that can spot and remove the little Trojans that infect our machines. Read my lips. If you have not done so, please download and run often the following programs: Spybot (www.spybot.com); Adaware (www.lavasoft.com); HijackThis (www.hijackthis.com). If your virus software has expired, either renew it, or download the AVG Free edition from www.gfi.com, which is some of the best anti-virus software on the market, and it is free. I have it on every computer I own. It works, and updates automatically. CNET ranks ZoneAlarm (www.zonealarm.com) the best anti-spyware on the market, although it will set you back $20. Or, go to www.nanoscan.com and have your computer checked for all viruses, Trojan horses, and other problems for free. It scans online and takes about an hour for a complete check, courtesy of www.panda.com. You don't have to sit and watch it, and it will scan in the background.

Finally, check your spam filtering software. It should have Bayesian filtering, and filtering for image/text embedded files. Consider the following for spam software if you

don’t have any or don’t like what you have: Zone Alarm Internet Security Suite 7, which is also ranked number one by CNET in 2007 for bundled security suite.

One last suggestion. Never, ever give out your personal or office email address when required to give an email address for an internet purchase or transaction. Create a personal email address at yahoo.com, which allows a user to create a “throwaway” address for use with internet purchases. All spam that results from a given email address is forwarded to your normal mailbox in care of your fake email address. When it is obvious that your fake address has become the spam attractor of the world, you delete the email address. Keeps your personal address clean. I have killed billions and billions of emails this way. Good luck.