Realtime publishers

"Leading the Conversation"

The Essentials Series

IT Compliance Volume II

sponsored by

SECURE COMPUTING

by Rebecca Herold

Addressing Image Spam

by Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI ***March 2007***

What Is Image Spam?

Have you noticed an increasingly large number of email messages coming into your inbox that have the text information imbedded within graphic images? Some of the most common types are those represented in Figure 1.

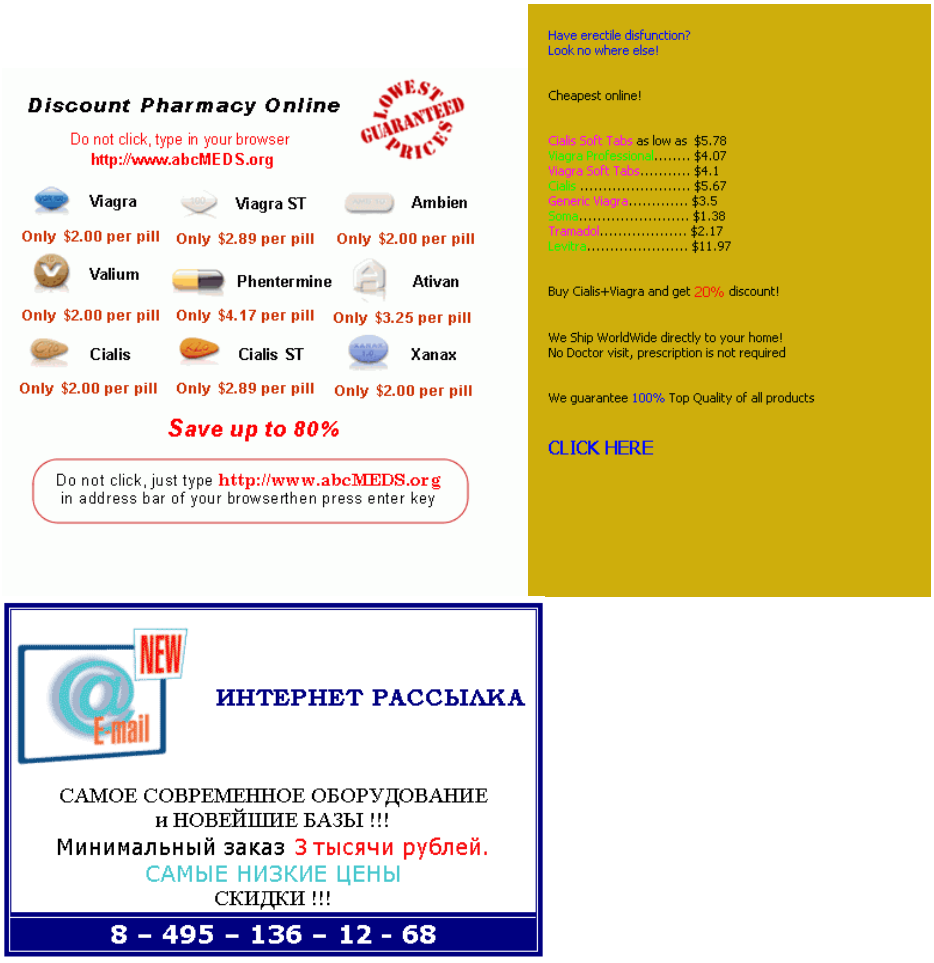

Figure 1.

> Another common image spam is one giving "hot stock tips." After the recipients bid up the price of the listed OTC stocks, the spammers then dump the stocks for a considerable profit.

The text portion of image spam frequently contains meaningless quotes from literature or copies of the latest news headlines, along with animated, tiled, oddly colored, and/or layered graphics that divide the message into multiple images stacked on top of each other. Many have even removed the typical links to click and instead direct the message recipient to type the URL into the browser; they do this because most filters look for the known malicious, clickable URLs within the email message.

According to Secure Computing research, the amount of spam has tripled throughout 2006, with a further 50% increase in just the first couple of months in 2007. Their research also indicates that spam now accounts for nearly 90% of all email, of which 30% is image spam.

Marshal's Threat Research and Content Engineering (TRACE) 2006 Report that was released on March 5, 2007 reported "Image spam normally accounts for 15 to 20 percent of all email but right now is accounting for more than 35 percent."

F-Secure indicates that "Image spam is taking up 70% of the bandwidth bulge on account of the large file sizes every single one represents."

Why has image spam become so popular? Because it is sneaky and effective for the spammers. Image spam defeats most spam filters. The clever spammers are fooling most spam filters by putting graphical text within an image so that the system doing the filtering just sees code, not the letters and numbers the recipient sees within the graphic.

Image Spam Negatively Impacts Business

Image spam can not only cause huge headaches to the IT folks but also bring a business to a halt if not addressed. Image spam is much more difficult to detect with conventional content analysis spam filters, is usually much larger than text-based spam, and takes significantly more bandwidth and storage. Image spam can flood your network and bring it to a standstill. If you depend upon your network for business processing, you could find yourself dealing with a non-responsive, spam-flooded network, with no access to your business applications or customers.

Businesses that rely upon their network for business success must address image spam and its negative impacts or suffer negative business impacts.

More sophisticated spam filters have tried to identify the letters inside graphics using optical character recognition (OCR) technology. However, the spammers have gotten wise to this and now have methods for outsmarting OCR. For example, they will use unusual fonts or put a lot of additional information and images, such as added color, gaps in letters, and so on, within the graphic so that the OCR does not recognize the letters.

Very generally, "botnet" refers to a collection of software robots, zombies, or bots that run on their own. Botnet can also be used to reference a network of computers using distributed computing software, typically some type of malware.

Another problem is that image spam and botnets are being used together. Botnets are what propagate most spam, but now botnets are also being used to alter a spam message image by changing the size, shape, colors, and so on so that it looks different to the filters that sort out identical emails.

As of October 2006, Secure Computing research identifies an average of more than 250,000 new zombie, or botnet, machines *every day*—an increase of 50% from only a few months earlier.

Addressing Image Spam Threats

Businesses must address the image spam problem to keep it from bringing their business processes to a grinding halt.

A few of the challenges for fighting image spam

- Multiple email servers and network entry points
- Overloaded email servers with outdated tools and monitoring
- Inadequate quality of email service

Some of the ways in which image spam can be addressed include:

- Use a single email server with a single entry point. Limit the ways in which image spam makes it into your network. Make sure all messages are scanned before they have a chance to negatively impact your network. Don't allow email messages to be accessed through Web-based mail systems.
- Use tools that analyze sender reputation. Is the sender known to have sent spam in the past? When was this sender seen for the first time? How much email is this sender responsible for? Does the sender both send and receive email, or only send emails? Is the sender's behavior sporadic or continuous? Is the sender on blacklists?

Sharp increases in sending behavior as opposed to a regular amount of inbound and outbound email, is one indicator of spamming. Senders who have an unusually high ratio of sent mail to received mail often are discovered to be spammers.

- Check the message reputation and fingerprinting. Does the message contain parts of previously received spam? Does a comparison of the image contained in the message contain similarities to known spam images? What are the network characteristics involved with the delivery of the message?
- Invest in effective, forward-looking technology. Vendors are working all the time to improve spam filtering, and image spam filtering in particular. It is not possible for your email administrators to keep out image spam using old methods.
- Review and update your email policy. If image spam is causing you particular problems or having a noticeable negative impact on network performance, consider blocking all attachments on incoming email. If this is not feasible, consider routing emails with attachments through a quarantine area for review first or allow only certain departments or groups to receive email with attachments if that is common for your business purposes.
- Keep your email systems updated. Image spam exploits vulnerabilities in unpatched email servers.
- Educate your personnel. First make sure they know the characteristics of what image spam looks like, then tell them to never reply to those odd-looking email messages, and not to click the links within them.
- Use your corporate lobbyists to strengthen government laws and industry policies. Make the penalties and fines for spamming more severe to help motivate these spammers not to continue with their disruptive messages. Doing so will also help keep marketers from trying to use image spam, as they are using it more because their other types of mass marketing messages are caught by the spam filters.

An interesting site with information about a wide range of spam types is the Spammer's Compendium (http://www.jgc.org/tsc/). It contains useful analysis for specific image spam messages.