Back to article Print this

Spam on the rise with new breeds

Researchers say spam has risen significantly in recent months -- by as much as 80 percent

By Tom Spring, PC World, IDG News Service

December 28, 2006

If you're like me, each morning you greet an e-mail inbox stuffed with a new breed of fiendishly clever spam that somehow manages to elude your spam filters.

Earlier this year we thought the good guys were winning the war against spam. Back in January, I talked to spam fighters who were claiming victory in the spam wars. One company told me that the volume of spam had stopped growing at double-digit rates for the first time.

But that may have changed. Researchers and IT managers are now complaining that spam levels have risen significantly in recent months -- some organizations have reported increases as high as 80 percent. Overall spam volume has increased 67 percent since August 2006, according to Barracuda Networks, an enterprise security appliance vendor.

So what's changed? How are spammers managing to sneak their messages back into your inbox? And what can you do to protect yourself?

New and Improved Spam

Spam used to be strictly text based and commercial in nature, touting herbal remedies, linking to porn sites, and coming from average-Joe spammers looking to make some extra money.

Spam fighters were able to block this type of spam based on key attributes, such as words and phrases typically found in spam. They could also block e-mail that came from a known spammer, or filter spam based on the links that the messages contained. If an e-mail contained links to a porn site, for example, then a filter might reasonably guess that was spam.

The new breed of spam manages to evade filters because it contains no suspect words, is sent from hundreds of thousands of different PCs, and includes no links. How does it work?

The new spam evades traditional spam filters because it doesn't include any text -- instead, it uses an image embedded in the body of an e-mail to deliver its message. This image includes text that displays the spammer's message. But to make it hard for spam filters that may use optical character recognition technology to scan and read the text in the images, spammers are getting sneakier. They're sending pictures with textured backgrounds or various colors to throw off the filters. They're also varying the font for each letter of the text.

This way a spam filter can't tell an unsolicited stock tip from a holiday picture of the family.

Image spam currently accounts for up to 40 percent of incoming e-mail, according to McAfee Avert Labs. A year ago image spam accounted for less than 1 percent of the total spam received, the company reports.

Pump-and-Dump Spam

The look of spam isn't the only thing that has changed. Much of the new spam no longer depends on people clicking a link or downloading a Trojan horse. Instead, the single purpose of most image spam today is to promote a specific company's stock -- it's a "pump and dump" stock scheme.

Here's how it works: People behind the scam typically buy a bunch of penny stock in a company. Next, they send out millions of spam messages touting that stock -- typically via zombie computers (owned by home PC users). When enough people buy the stock -- and believe it or not, some people actually do -- the spammers sell their holdings and make a modest return.

How many people actually fall victim to these stock tips? A spammer can make a 5 to 6 percent return in just a few days from stock hyped via spam, according to a recent study conducted by researchers at Oxford University and Purdue University. The researchers also found that spam recipients who invest in those same stocks lose about 7 percent of their investment.

These types of pump-and-dump spam stock schemes are growing exponentially on the Web, according Stephen Pal, vice president of product management for Barracuda Networks, an enterprise security appliance vendor.

Organized Crime

The recent explosion in image spam that hawks penny stocks is likely the work of Russian hackers controlling an army of botnet PCs, says Joe Stewart, senior security researcher at SecureWorks. A botnet is a network of hijacked PCs that forward spam or viruses over the Internet to other computers without the knowledge of the zombified PC's owner. As many as 100,000 PCs make up this army, and they're probably seeded with the SpamThru Trojan, Stewart says.

This botnet army is very advanced, Stewart says. The SpamThru Trojan scans a PC for viruses and removes competing malware files, he says. Once a PC is infected, it becomes a zombie controlled by a central server. A botnet army this large is capable of sending a billion spam messages a day, Stewart says.

Our best hope for stopping the scourge of image spam rests with the spam fighters. One way you can help is by giving feedback to your e-mail provider. Companies like Barracuda Networks and e-mail providers like Google Gmail and AOL ask that their customers identify the spam they receive by pressing a "this is spam" button, rather than just hitting Delete. This feedback helps companies prevent the same messages from reaching other inboxes.

Chasing down the spammers is as futile as investing in the penny stocks they promote, experts say. Right now resources for fighting spam are best focused on protecting people -- not going after the bad guys, Stewart says. "The fact is that law enforcement doesn't have the authority or resources to track down spammers," Stewart says.

That leaves little hope for those of us on the receiving end of spam. For now, all we can do is make sure our antivirus and antispam software is up-to-date.


Print this