Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

How spam vigilantes are wrecking email and encourage violations of law

To counter the deluge of unsolicited commercial email (UCE), the anti-spam community has brought groups of people to the world who, without legal basis, and out of a belief that stopping "spam" is more important than protecting the rights of others, have acted as vigilantes to try to stem the tide of these emails. Along the way, they have:

- Broken email mechanisms that are at the heart of Internet communications.
- Caused major operational problems for companies and individuals.
- Caused about 100,000 people each day to be unable to send email to others.
- Led criminals who send illegal unsolicited commercial emails to perpetrate frauds to break into more computers, use harder to detect techniques, and increase the complexity of defending computers for all the rest of us.

They know that they do this damage to others, hide behind anonymity, lie about the reliability of their mechanisms, and pride themselves on inconveniencing others to get their way. If you want to get legitimate emails from people like me, either you have to stop using their mechanisms or I have to cause my computers to lie to you,

This is how you or others like you are contributing to their cause and disrupting yours and others' emails by helping them out.

The anti-spam community has vigilantes:

A vigilante is typically defined something like: a person who takes the law into their own hands by avenging a perceived crime. Avenging, as in getting even, or doing something they think will get even, a perceived crime, such as sending unsolicited commercial email, and taking the law into their own hands, as in not using the available legal means, but rather acting outside of the law. Take for example, Spamhaus:

- This group acts across national borders and uses the national laws to avoid legal actions against them.
- They are people who use pseudonyms to avoid having others know who they are because, according to them, they are afraid of retribution.
- They use secret sensors that they won't reveal details of because, they claim, then they will be avoidable by the spammers.
- They organize as a cell structure, just like any insurgency that is well trained will do.
- They assert that some of their mechanisms cause about 100,000 people every day to have their emails blocked because their detection methods produce false positives.
- They have been responsible for cutting off communications for large companies because those companies happened to be using the same IP address range as ISPs

whose customers sent what Spamhaus thought was unacceptable content.

- They put false statements on their Web site about the causes of blacklisting sites.
- They intentionally make it difficult to figure out why your emails are not getting through.
- They don't provide any notice to those they are blacklisting.
- Their blacklists are widely distributed and used by innocent third parties who believe that they are doing the right thing.

They know that these things are true. Even after I pointed these things out to them, they continued to act in this way, even with regard to addresses that they have repeatedly caused to be blocked, even after they had notice that they were inappropriately blocked, and even when they knew they were interfering with legitimate communications. They indicated that they have considered stopping this knowing interference with others because of the damage it causes, but that they decided to continue it anyway because they think that it is worth harming others to fight against "spam".

How does this force legitimate emailers to lie?

In order to get my emails to you and other folks on the Internet, at least to sites who use the sorts of filters that use the false positive detections put forth by Spamhaus and others like them, I have to configure my computers so that, instead of following the Internet RFCs and standards, they violate those standards. No kidding. I have to configure my computers to lie about their names when they send emails in order to avoid triggering the detectors out there, because if I don't, the filters will detect the truthful information my computers normally send as an indicator of "spam" and instruct the many thousands of companies who use these mechanisms to stop UCE.

And the effect on the criminals:

Of course the criminals have no problem with lying, cheating, or stealing. So when the vigilantes use their techniques that harm legitimate email senders, they don't really do any significant harm to the criminal email senders. The criminals just escalate their tactics. And what tactics have they adopted? They now break into millions of computers at a time with worms and viruses, use those millions of computers to send their frauds and sublease them to others to send emails of various sorts, and when the vigilantes try to shut them down, they just break into a few million more computers. The anti-spam vigilantes are making the criminals into bigger criminals by forcing them to get better at doing more illegal things that harm more people in order to send their emails.

Now there is a legitimate argument to be made that it's not the fault of the people who try to stop crimes that the criminals get better at committing them. But that argument falls away when the people trying to stop the crimes are acting outside the law themselves. There are legal means for stopping crimes and legal means for making actions criminal if you think they should be criminal. But the law does not work at the speed that most of the Internet technical crowd would have it work at, so we get vigilantes.

What can you do about it?

There are many legitimate sources of detection mechanisms for various sorts of unsolicited commercial emails as well as other content that is undesirable based on your personal or corporate view. If you want a law abiding society and you want to continue to have freedom of speech, you should be using these legitimate sources and paying them an appropriate fee for their services - assuming you don't want to get these emails. If you contribute to a vigilante group, you might also find yourself at the wrong end of a legal action, because now that you have read this, you are on notice that helping the vigilantes might constitute interference with legitimate commercial and individual activities, and this might be a tort on your part.

The two main ways that people contribute to these groups are by

1. Providing them with data, sensors, or other similar assistance,
2. Paying them.

If you stop doing this, they will stop doing what they do.

How do you tell a legitimate company from a vigilante?

Telling a vigilante from a legitimate anti-spam company is not that hard. Here's a list of things you might consider:

- Only deal with companies where the people have real names and addresses and the company has a real address. If you don't know who they are, and they won;t tell you, chances are very good that they are illegitimate.
- Only deal with companies that you have done a background check on, especially if you are providing them with information that you gather or use their sensors in your network. Remember you are granting them access to your traffic flows and potentially your systems through the software you place in your infrastructure.
- Don't do it without a contract! If you don't have a legal contract approved by the legal department, you are taking a legal risk with your job or your business.

Of course in many cases, these sorts of capabilities are put in place by well-meaning employees. But just because they are well meaning doesn't mean they are right or that you won;t be held liable for their actions. From a company perspective, you should make certain that you don't let this happen except through official channels. It might violate regulations, laws, policies, or work rules, and if might produce law suits against your company or prevent you from being as successful in business.

Audits should also look for indications of the use of such services without the legal contracts in place, because there may be other legal and business implications. Such systems tend to violate standards, such as ISO 27001 and 27002, don't usually have proper change management and corporate maintenance in place, and become problematic when managed across large numbers of systems.

I am looking forward to a lot of spam regarding this article. After all, one of the main tactics of the anti-spam vigilantes is to sign up the people who oppose them to high volumes of spam.