

22 Things a Domino Administrator needs to know about spam—An interview with a spammer.

Times were that spam was just a nuisance. Now spam is at the root of electronic crime, corporate espionage, phishing, and theft. If you don't control spam completely, your company, servers, and people are at risk. The following articles will give Domino administrators insight into the shady world of spammers through a 2-part interview with a spammer and an informative article. Read this and learn.





22 Things a Domino Administrator needs to know about spam—An interview with a spammer.

Table of Contents:

[Answers and advice from 'the spam man'](#)

[Revelations from a reformed spammer](#)

[Online crime as ugly as ever](#)

Answers and advice from 'the spam man'

By Christine Polewarczyk, Senior Editor
SearchDomino.com

"Spammer-X," reformed spammer and author of the book, *Inside the Spam Cartel*, offers advice to SearchDomino.com readers on how to effectively fight spam.

SearchDomino.com member: Looking at the raw header of a message, is there a way to track the message back to the originator?

Spammer-X: You could trace it back to where the mail came from, but that may be a compromised machine, and will probably not be the address of the spammer. So no, there really is no way to track a spammer down by looking at headers.

SearchDomino.com member: My company has zero tolerance for false positives, but complains about the spam we have been receiving since I was told to turn off our filters. Do you have any suggestions? I know it's sort of a Catch-22.

Spammer-X: Yes, it's a Catch-22 all right. Bayesian filters will help with this, filters that only mark spam if you personally declare it spam. Try network-level filters, deny mail sent from DSL and cable, and use other filters that do not rely on content base. But, really, you should run all filters and just tune them correctly. If your company is really worried, try only flagging spam as spam, not deleting it.

SearchDomino.com member: How can a company block foreign-language spam?

Spammer-X: Look for foreign characters, or a character set that identifies Unicode or some other non-English setting.

SearchDomino.com member: Do botnets set up SMTP servers on compromised machines and then retrieve spam from a centralized or decentralized "server"?

Spammer-X: No, usually they only act as entry points for a spammer. As dumb mail relays, they are only there to hide the source IP address, like a proxy server.

SearchDomino.com member: What is the best way to detect a botnet working within a LAN?

Spammer-X: You need a virus scanner on each machine. Also, run a sniffer on the port and an intrusion detection system on a spanning port. That's a good start.

SearchDomino.com member: How does a hacker control who uses his botnet?

Spammer-X: Usually, each client in the botnet will connect to an IRC server and sit in a channel. They take commands from a master (who has the password). The master can set up the clients to accept spam for delivery or change the port they listen on.

SearchDomino.com member: How successful are real-time blacklists, such as spamhaus in the fight against spam? Is this a changing trend?

Spammer-X: They help, but botnets really disable them. When you have 30,000 new hosts sending spam, it can take a while for those hosts to be added to spamhaus. This is why botnets are so popular.

SearchDomino.com member: Do you have a favorite DNS blacklist providers or are they not reliable?

Spammer-X: Use them. Use every one available.

SearchDomino.com member: What's the purpose of sending spam that is full of garbage/unreadable content?

Spammer-X: To bypass content-based, keyword filters. Spam that has many 'passive' words, such as "Jack the rabbit went to the store 33 2003-Jan," looks more legitimate, even if it contains "Buy Viagra here." It's to beat a frequency analysis.

SearchDomino.com member: I still am not sure as to how the e-mail lists are getting out to the spammers. Do they attack e-mail servers directly to harvest the e-mail addresses? Are there certain SMTP commands that should be blocked?

Spammer-X: Well, yes, some try traversals, like trying to deliver a message to A@user.com, b@user.com, etc. This can be stopped with tarpitting, where each sequential message takes a longer time to be delivered. However, a majority of spammers just hack into mail servers or subscription programs and steal the subscribers. It's easier than you think.

SearchDomino.com member: I notice most spam is only a few K, but I am also seeing more and more spam that is upwards of 30 K. Is size becoming less of a barrier?

Spammer-X: It's harder and there is more setup cost involved, but the returns are greater for the spammer. I think the wide penetration of broadband has given spammers access to more bandwidth. This is why you're seeing larger spam being sent.

Revelations from a reformed spammer

By Christine Polewarczyk, Senior Editor
SearchDomino.com

Continuing from part one of this two-part article, Spammer-X, reformed spammer and author of the book, Inside the Spam Cartel, answers more of your spam-related questions.

SearchDomino.com member: What do you think about Bill Gates' declaring spam would end inside of one year?

Spammer-X: I say Bill is just angry about getting so much spam himself. I would like to see him stop all spam within a year. That's like saying Windows won't crash. Yeah right. I don't think spam will stop anytime soon.

SearchDomino.com member: Do you find the current laws regarding spam are getting better -- for example, the recent spammers who got convicted to nine years in jail? What future solutions do you see regarding antispam?

Spammer-X: Yes, jail time works well. It sends a clear message into the spam community and many people really think twice about sending spam. However, I think the jail times are too strict. Spammers can get jail sentences longer than a rapist; it does not seem just somehow.

SearchDomino.com member: Do you know the SPF (Sender Policy Framework) initiative? How are spammers dealing with it?

Spammer-X: Yes, I know it well. Spammers can easily get around it. It makes a spammer accountable to a hostname, or a hostname with an SPF record. Just register a hostname, set up an SPF and you're away laughing. Recent studies found that there is more spam with SPF records than there is legitimate mail.

SearchDomino.com member: What happens when I elect the "opt out" option offered in many spam messages? Is this a technique spammers use to validate e-mail addresses, and therefore propagate, rather than remove, my e-mail address?

Spammer-X: Yes, this is usually used as a method of validation.

SearchDomino.com member: Is there any way to check to see if you are part of a spam database?

Spammer-X: Sure, that's easy. Do you get spam? If yes, then you're in a spam database.

SearchDomino.com member: Are whitelists at mail sites being compromised or is it educated guesses?

Spammer-X: They are being compromised. I actively did this as a spammer.

SearchDomino.com member: When you mentioned complaining to the credit card company, how would you go about doing this?

Spammer-X: Make it as scary as possible. It's easier for the credit card merchant to just can the account of the spammer. Here's a rough example:

Dear X: One of your clients sent my company spam -- spam that is considered illegal under U.S. jurisdiction. Attached is a screenshot of the spam and list of the headers. His Web site, www.fake-pills.com, is using your company to bill credit cards. Legal action will be filed if this spam continues.

SearchDomino.com member: Did you ever deliver your spam with the well-known NET SEND vulnerability?

Spammer-X: Negative on the NET SEND. It requires the recipient to have both NetBIOS and RPC open for you to connect to. Because of all the DCOM worms going around, most people now run firewalls, which blocks any attempt to use NET SEND.

SearchDomino.com member: If a spammer/phisher installs a mailer on your server and you kill it later (after everyone blacklists you), do they generally attempt to reinstall it or just move on to an easier target?

Spammer-X: The mail server would have had to be someone special. When I was spamming, if the host was blacklisted, I would have given up. There's no point flogging a dead horse.

SearchDomino.com member: What kind of antispam technology does the spam-fighting software you are developing use? When will it be available?

Spammer-X: It's based on a new variant of a Bayesian filter, using bi-linear trend analysis. I hope to have the product ready in 2006.

Online crime as ugly as ever

By Victor R. Garza, Contributor
SearchSecurity.com

MOUNTAIN VIEW, Calif.—According to the keynote speaker at this year's Conference on Email and Antispam (CEAS), spam is still driven by bands of underground Internet miscreants driven by a lust for money and mischief.

Rob Thomas, CEO and research fellow with Internet security think-tank Team Cymru, opened the third annual gathering of antispam researchers and software engineers with a lively presentation on the 'underground economy.'

Thomas said in his work with clients he has come across villains who are driving a mature and robust economy that continues to expand.

"It's grown well beyond [credit] cards, warez and porn... now you can get everything; credit cards, CVV [credit card verification numbers], bots, bot code, DoS nets" and even U.S. visas, birth certificates and passports, which can go for as much as \$500 each.

Thomas went on to describe the early union of spammers and bot herders, a term for individuals who use scores of machines running automated software to distribute spam, generating a substantial revenue opportunity for spammers and created the myriad of email headaches that network administrators face today.

Today Thomas said the underground economy is rife with data stolen and traded illegally in much the same way that traders in a bazaar or flea market sell their wares. In fact, he said, stolen data is costing businesses in the UK \$150,000 in U.S. dollars each hour.

Included in this information Thomas said are "fulls" or fully identifying information of distinct victims including names, addresses, phone numbers, mother's maiden names, Social Security numbers, secret questions, secret answers, banking information and more. While credit cards may not be quite as alluring as they once were, numbers from the major credit cards firms are available, including Visa, MasterCard and Discover and even the coveted American Express Centurion cards, "they love those, and yes, they do trade them".

Thomas went on to talk about the communication methods used by these miscreants to interact including a variety of different instant messaging, peer-to-peer and stolen Skype VoIP accounts. He said the Skype accounts used to conduct miscreant business are usually used in pairs and, once used, are disposed of.

Most online criminals, according to Thomas, by and large are not all that tech savvy, and for them "it's not about technology, it's about crime," since most of these individuals were "selling drugs on the street and then found that it was a lot easier to clean out bank accounts from their La-Z-Boy."

And when it comes to online fraud, spammers aren't strictly interested in credit cards. Thomas said online banking accounts are just as susceptible to subversion and hijacking. He pointed out that access to a bank account containing roughly \$3 million dollars had been sold from one criminal to another for just pennies on the dollar.

While the bank in question compensated the victim, in this case Thomas pointed out that someone with that much money has pull with the bank, "but if it had been someone with \$800, which we more commonly see, what does the person with eight hundred bucks have in the way of clout?"

Thomas noted out that it's a problem that isn't going away. "People are getting nickeled and dimed, but for these people nickels and dimes are all they have."

Victor R. Garza is a technology/security consultant and lecturer at the Naval Postgraduate School in Monterey, Calif.