

Evolving Methods for Sending Spam and Malware Panel: Spammer Requirements and the Spam Ecosystem

**FTC Spam Summit: The Next Generation of Threats
and Solutions, July 11-12th, 2007, Washington DC**

Joe St Sauver, Ph.D. (joe@uoregon.edu or joe@internet2.edu)
Manager, Internet2 Security Programs, Internet2/U of Oregon
<http://www.uoregon.edu/~joe/spam-summit/>

Disclaimer: all opinions expressed in this presentation
are strictly the author's, and do not necessarily represent
those of any other organization or entity.

The evolution of spam: it ISN'T exclusively a "technology thing" anymore

- While it would be easy to focus **exclusively** on evolving technological spam phenomena (such as the move toward sending image spam to avoid SURBL filters, or emergence of fast flux hosting as a phenomena), **the evolution of spam and spamming ISN'T just a "technology thing."** Spam is also evolving at "strategic" and "business" levels.
- For example, illegitimate **affiliate programs** allow spammers to efficiently scale up/"franchise" their operations horizontally while also providing additional "insulation" from prosecution ("hey, I **told** my affiliates not to spam!").
- In fact, we're seeing the emergence of a specialized "**spam ecosystem**," comprised of specialized suppliers of goods and services for spamming. Result? Higher efficiency & a lower bar to entry (buy rather than build what's needed), etc.

That ecosystem is complex (AND vulnerable!)

- Because spamming is an increasingly sophisticated, complex and collaborative activity, it largely isn't something which a spammer can learn and then do on their own anymore. New spammers need to comprehend a continually expanding body of operational techniques ("**spam tradecraft**") in order to efficiently deliver spam while avoiding filtering, civil suits and criminal prosecution.
- Learning that spammer tradecraft, and doing routine spam-related business, requires spammers to **communicate** with others spammers, and with spam support businesses. Monitoring those communications (with appropriate court permission) may make it possible for LE to use traffic analysis to identify participants in spammer organizations.
- Spammers also need to make **purchases** of spam-related goods & services (colocation space, etc.), potentially leaving behind incriminating financial records for forensic review. ³

Following that money trail

- The U.S. Money Laundering Threat Assessment Working Group did an great job of describing the financial channels which miscreants exploit; I'd urge everyone to review the Dec. '05 **U.S. Money Laundering Threat Assessment**, <http://www.ustreas.gov/offices/enforcement/pdf/mlta.pdf>
- Not surprisingly, in view of that scrutiny, financial choke points are beginning to emerge. Spammer **payment processing** is a prime example of this. For example, at least in the case of one popular pharma spammer, only **one** type of credit cards can still be used by customers to pay for illegal controlled substances. Identify a way to break THAT financial channel, and spammers will be badly damaged.
- Or scrutinize the payments made by affiliate programs to their participating affiliates. Are **income tax liability issues** associated with that income stream being properly handled?

Follow the product (order fulfillment)

- If you're chasing connections between spam, spammers and spamvertised products, don't forget that spammers need to get spamvertised products to customers -- unless spammers are just directly defrauding their customers. (After all, if a spammer **does** rip off a customer, would the customer really complain to local police that they're not receiving the illegal controlled substances they've purchased online?)
- Assuming spammers **are** delivering some products which people order, those products are getting **shipped** from somewhere, probably via a major common carrier. Records/patterns are being created—but is anyone looking at them?
- There are no borders in cyberspace, but there **ARE** borders in real life. When spammers ship illegal drugs from abroad, those shipments go through **customs**. If you want to disrupt pillz spammers, seizing shipments at the border is a great step – but does Customs (and DEA) have the needed staff⁵?

Spammers and anonymity

- As spammers see things like financial and fulfillment channels being successfully attacked by law enforcement, not surprisingly, spammers adapt. That's one reason why smarter spammers now prefer to spam things which can't be directly tied back to them, such as **stock pump and dump spam**, or **mortgage lead spam**. Spammers are looking for insulation. Spammers are looking for anonymity.
- There are plenty of things which help spammers in their quest for anonymity, including:
 - anonymized domain registrations (to say nothing of the ongoing problem of completely bogus whois contact data)
 - cheap/easy-to-create offshore shell corporations,
 - national privacy laws (particularly in some parts of the EU) which interfere with even voluntary action by ISPs to protect their own facilities/customers from exploitation, &
 - primitive mechanisms for international LE cooperation. ⁶

Spam: it /S an INTERNATIONAL phenomena

- As the United States cracks down on spam, spammers are developing an increasingly strong affinity for Europe, including living in Europe, exploiting European consumer PCs to send spam to United States email addresses, etc.
- Because spam is an international phenomenon, dealing with spam will require a coordinated **international response**. It doesn't help much if we clean up all our domestic spam zombies, if we're still getting hammered by spam sent through Poland or Spain, or if spammers have a safe base of operations in Russia or elsewhere overseas.
- Some may even go so far as to describe spam as a sort of low-intensity cyber warfare conducted via third parties. **How much in aggregate has the US economy been damaged by spam?** What a "perfect" way for those who hate the US to safely attack our economy! We may not even notice we're being attacked, and if we did, how would we respond?

Six Quick Closing Thoughts

- 1. The Internet is a gigantic laboratory for spammers. They can easily try new approaches and see what works. While we can and must respond to any and all of those new approaches, we're never going to win if we just play a defensive game since it always take time to develop and deploy countermeasures. **We need to go on the offense.**
- 2. **Spamming requires a lot of "stuff."** Spamming is not a lightweight activity, and there's a substantial specialized industry of folks who've grown up around spamming, all doing business supporting it. ALL of those cottage industries can and SHOULD be targeted for investigative attention.
- 3. **Choke points exist, and they need to be worked relentlessly.** Merchant account processing and interdiction of illegal shipments at our borders are excellent examples of these weaknesses.

- **4. Spamming activity doesn't occur in isolation.** For example, spam senders communicate with, and are paid by, affiliate programs. If you can bust spam senders you can use them to identify affiliate programs; if you bust affiliate programs, you can use them to work back to spam senders. When you uncover one thread, follow it to find all the rest of the operation, and offer deals (including immunity from prosecution) to get the little guys to roll over on the big guys.
- **5. The bad guys have learned one key lesson of the Internet: they're doing an excellent job of **scaling up** their operations, with affiliate programs being a prime example. Does the U.S. **also** have plans to **scale up** *its* **anti-spam** operations? **What's next, post CAN-SPAM?****
- **6. Spam is an international problem** and one which will require a coordinated **international response** if we're going to win. The United States must show international leadership and support for international antispam efforts. ⁹