Infected PCs Acting As Spam Zombies: We Need to Cure the Disease, Not Just Suppress the Symptoms

2nd Joint London Action Plan-CNSA Workshop

International Enforcement Cooperation:
Spam, Spyware and other Online Threats
December 13, 2006, Brussels, Belgium

Joe St Sauver, Ph.D. (joe@uoregon.edu)
http://www.uoregon.edu/~joe/lapcnsa2/

Disclaimer: All opinions expressed are solely those of the author and do not necessarily represent the opinions of any other entity.

Alternative formats: This talk has been provided in both audio narrative format and as a written transcript for ease of indexing and full accessibility.

Despite all our ongoing efforts…

- The spam problem continues to worsen, with nine out of every ten emails now spam. [1]
- Spam volume has increased by 80% over just the past few months, [2]
- And users face a constantly morphing flood [3] of malware trying to take over their computers.

- Bottom line: **we're losing the war on spam.**

The root cause of today's spam problems is spam zombies, with 85% of all spam being delivered via spam zombies. [4]

The spam zombie problem grows worse every day

- For example, TrustedSource mentions that they identify "nearly 250,000 new zombies [...] each day." [5]

- **That's over ninety one million new spam zombies per year.**

- **If anything, I believe that estimate is significantly low.**

Users don't, won't, or can't clean up their infected PCs…

- Some may not even know they're infected.
- Others may **suspect** something's wrong (for example, their computer may suddenly have become slow or may suddenly have begun to act strangely)
- ***BUT*** many users don't have the interest, time, expertise, or antivirus software they'd need to clean up their computer.
- Many users are also unwilling to pay someone else to do that cleanup for them.

ISPs can't be expected to clean up their infected customers' PCs

- Helping a customer to manually disinfect and harden a system can take hours
- Each ISP may have thousands of customer systems which need disinfecting
- Additional customers are constantly being newly infected; support never catches up!
- Profit margins per customer are too slim to allow ISPs to clean up systems for free
- Post-cleanup issues, if any, will invariably get blamed on the cleanup process

So what are some ISPs doing?

- Some ISPs have begun to filter outbound email traffic from their customers' PCs.
- A common example of this is filtering port 25, which eliminates the ability of customer PCs to act as so-called direct-to-MX mail servers in their own right.
- Customers *can* still send email from their PCs, they just need to route that outbound email through the service provider's officially approved SMTP servers.

Filtering Port 25 and Rate Limiting

- When an ISP begins filtering port 25, they also usually simultaneously "rate limit" the amount of email each customer can send via the ISP's official email servers.
- By rate limiting each customer's outbound email flow, the ISP insures that even if a customer's computer does get zombied, it will only be able to emit a trickle of spam.
- This, along with helping users to get cleaned up, is a BCP established as part of *Operation Spam Zombies.* [6]

Unfortunately…

- Filtering port 25 and doing rate limiting is like giving cough syrup to someone with lung cancer -- it may suppress some overt symptoms but it **doesn't cure the underlying disease.**
- Filtered and rate-limited spam zombies **CAN still be used for <u>many, many</u> OTHER bad things, and they represent a <u>huge</u> problem if left to languish in a live infected state.**
- Let's consider 5 brief examples.

1. DoS attacks

- Filtered-but-not-cleaned up spam zombies can end up being used to conduct denial of service (DoS) attacks, flooding an attack target with unsolicited traffic.
- DoS attacks have taken down some of the largest and best known sites on the Internet, notwithstanding carefully planned DoS mitigation strategies.
- DoS attacks have also targeted key Internet resources, such as root name servers. [7]

2. Sniffing traffic

- Another risk is “sniffing” or eavesdropping on network traffic, perhaps capturing sensitive personal information, confidential financial data, or username/password pairs…
- Even if a zombied host doesn’t sniff traffic, the malware on a zombied computer can still provide a “back door” through which bad guys can rummage around in local and network drives. Anything sensitive right there on that system, maybe?

3. Scanning for vulnerabilities

- Another possible misuse of filtered-but-not-disinfected zombies is scanning for **additional** exploitable hosts to 0wn.
- This is a “leverage-based” strategy, the online equivalent of “using one gun to get a whole arsenal's worth more.”

4. Hosting illegal content

- Another undesirable possibility is web hosting on zombies (this is often referred to as "fast flux hosting").
- If you have illegal content that you can't host on a legitimate web server, such as
  -- viral web pages,
  -- child porn,
  -- pirated software, or
  -- phishing web sites,

  those pages may end up being delivered via spam zombies acting as web servers.

5. Click fraud

- The Internet relies on pay-per-click (PPC) advertising to support access to web based services such as Google.
- Click fraud undercuts that key business model by substituting automated “clicker software” running on zombied computers for real shoppers, thereby making money for the click fraudster at the advertiser's expense
- If advertisers lose confidence in the integrity of PPC advertising, ad-based financing for key web resources may end up in jeopardy.

Let's face reality: we're in the middle of a worldwide cyber crisis

- It is time for a **new strategy**…

  an international governmental strategy that is **commensurate** with the extreme levels of spam and compromised systems we're facing…

  a coordinated international **cyber crisis response plan** that's appropriate for a true **cyber epidemic**…

But do we even have a cyber crisis response plan for spam?

If so, it is TIME to execute it
or completely rewrite it,
because we're being overrun.

The general public…

- Still doesn’t know that most spam's being sent via infected computers
- Nor do they know that THEIR computer may be infected, or HOW to fix their system if it is infected, or how to avoid getting RE-INFECTED
- **An education campaign is an essential part of any cyber response plan.**
- Heck, a simple question: where's even basic TV coverage of this critical issue?

Once users learn that they have a problem, what do we tell them to do?

- Most infected users are non-technical.
- Non-technical users need a simple, scalable, “one-click” solution they can get and easily run to clean up their computer
- It is common for universities to produce and distribute a one-click clean-up-and-secure CD for use by their students and faculty.
- It's now time for our **governments** to produce and distribute an equivalent disk for **everyone to use**.

A CD????

- Yes, a CD.
- Some infected PCs may be offline and no longer have Internet access, or PCs may be infested with malware which prevents those PCs from accessing common online disinfection resources.
- Other PCs are connected only via dialup, and it would take too long to download and update those PCs over a modem.
- CDs, on the other hand, will work virtually everywhere.

Some one-click cleanup disk FAQs

- **Q. How would you distribute the disk?**

  A. Via post offices, primary and secondary schools, convenience stores, etc., etc.
- **Q. What antivirus product would be used?**

  A. Produce multiple versions using different antivirus products, and let users pick which one they want. Avoid monoculturalism.
- **Q. What would this one-click disk cost?**

  A. The disks would be free, underwritten and distributed at no charge by the government.

Who will provide help beyond what a one-click disk can do?

- The key to scalably dealing with over ninety million compromised systems a year is doing a flawless job on the one-click cleanup disk, thereby minimizing the need for time-consuming manual assistance.
- When manual assistance is genuinely needed, I believe countries should be fielding non-law-enforcement-based cyber emergency public health teams, analogous to the medical emergency public health teams deployed by the CDC or the WHO.

Financial assistance will also be needed

- Purchase of new systems is key to getting old impossible-to-secure systems offline
- As an incentive, governments should provide a tax credit for up to **half the cost** of a basic, more secure, current-generation computer.
- That tax credit should be capped at the equivalent of US$250 per system, only be available once per taxpayer, and require that an obsolete system be surrendered for disposal within 30 days of the purchase of the new replacement system.

International assistance

- While many spam zombies are found in the G8 countries, many others are not. Thus, we cannot reduce spam to acceptable levels through solely domestic efforts – we need a coordinated **international** response.
- Moreover, because some spam zombies are found in developing countries where resources may not be available to tackle cyber issues such as spam zombies, suitable financial and technical support for our international partners will be a key part of any spam cyber crisis response plan.

“All that sounds expensive!”

- Compared to the chronic economic impacts of spam (to say nothing of the even greater potential costs of mass scale cyber attacks enabled by filtered-but-still dangerous spam zombies), an international anti-spam cyber crisis response program consisting of user education and outreach efforts, a free clean-up-and-secure CD, a $250 computer tax credit, creation of the cyber equivalent of the CDC, and some foreign "cyber aid" actually sounds like a **tremendous bargain** to me!

In conclusion

- Much more needs to be done to resolve the current cyber crisis, but fully describing such a program of work is really more than we can cover in the time available today.
- Thank you for the chance to share a few thoughts with you, and please note that the endnote references found in the body of this talk correspond to the sources shown on the slide after this one.
- Feel free to contact me by email if you have any questions associated with this talk.

- [1] http://www.postini.com/news_events/pr/pr110606.php
- [2] http://www.toptechnews.com/story.xhtml?story_id=1230048NUTPO
- [3] http://news.moneycentral.msn.com/ticker/article.aspx?feed=BW&date=20061017&Id=6109299&symbol=US:CTCH
- [4] http://news.moneycentral.msn.com/ticker/article.asp?Feed=BW&Date=20061017&ID=6109299&Symbol=US:CTCH
- [6] http://www.ftc.gov/bcp/conline/edcams/spam/zombie/
- [7] http://www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf
- [8] http://www.computerworld.com/blogs/node/3679