Short Paper Review of:

**The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns**

**Citation:**


**Author(s) Affiliation(s):**

- University of California, Santa Barbara
- Ruhr-University Bochum
- LastLine Inc.

**Claims:**

- Presentation of a “comprehensive” analysis of the cutwail botnet from the botmasters perspective.
  - The study was made possible due to the authors access to actual C2 servers.
- Examine how modern spam campaigns are managed / delivered.
- Analyze the underground site spamdot.biz

**Likes:**

- I liked that they used a different Botnet other then storm for their research, it was a nice change of pace.
  - The malware responsible for the botnet is distributed via email and drive by download
    - Using the Zeus trojan as part of the botnets spam campaign was done during tax season and focused people looking for income tax advice. (Focused / Intelligent Spamming)
- They estimate and point out that their estimates on the size of the botnet is just an educated guess.
- Each C2 server increments the bots identifiers individually so estimation can only be done on a single C2 server basis.

- I found the statistics on how many email addresses are viable versus not to be amazing. The 1.7 Trillion sent and only 500 Billion being successful is astonishing. Given the magnitude of the number of sent messages it's amazing we don't see more spam.

- I was surprised at the ease of use that the botmasters have built into this particular botnet. The idea that they have built a web interface for users who rent the botnet is surprising enough. But more so the fact that they added a copy of spamassasin to check to see if the spammers spam will make it though or not before attempting to send is really interesting.

- The level of sophistication of the botmasters is extensive, this proves that this is an extensive business if they have the time to write a user manual.

- Interesting that the Asian bots were just as successful as the US based bots. I wonder why they are cheaper if they are just as effective?

- I was happy to see that they explained their system of data-collection that resulted in them finding cutwail. I was surprised that that the ISP's were willing to share copies of the C2 servers after the takedown to the university.

Dislikes:

- This is my number one complaint:

  - They claim to have obtained a copy of an underground forum known as Spamdot.biz. What exactly does that mean? Did they get access to the forum or get a ripped copy of it? How did they get access to it?

    - I think this is important to know since a lot of the economical conclusions are made from analyzing this forum.

Repeat / Add to Work?

- I was really surprised at the level of sophistication of the botmasters. This paper really surprised me with many of the things that the authors were able to find. My only complaint was about them not describing how they got access to the underground forum.

- I could totally repeat this work. This was very interesting and would be more so if we could setup a similar system and look for perhaps a different type of botnet to analyze.

- I think we should keep this one as an on-going potential topic that we could weave into some of the other Honeypot and Botnet analysis work.