Spamcraft: An Inside Look At Spam Campaign Orchestration

Christian Kreibich, Chris Kanich, Kirill Levchenko, Brandon Enright, Geoffrey M. Voelker, Vern Paxson, Stefan Savage

Proceedings of the 2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '09), Boston, Massachusetts

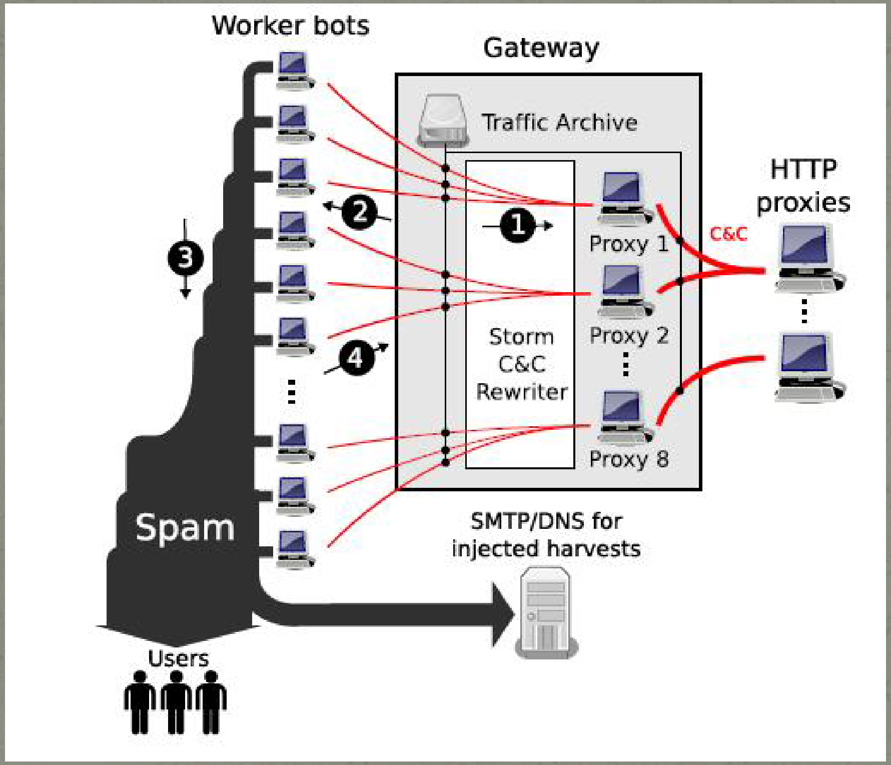
Presented by: Geoffrey Ong

Summary

"…spammers must gather and target a particular set of recipients, construct enticing message content, ensure sufficient IP address diversity …, and maintain sufficient content diversity…"

- Infiltrated spamming campaigns hosted on the Storm botnet.
- Study of:
  - Targeting strategies
  - Usage patterns of domains
  - Harvested email addresses
  - Target group selection / target list maintenance

Appreciation



Appreciation

- Collected and presented a large dataset.
  - Spam templates, timeframe, number of harvest email addresses, campaign types… etc

- Useful for further research if applicable.
  - Able to compare statistics with other studies

Critique

"The ability to identify test campaigns can provide crucial information on law enforcement, since it points out email addresses directly connected to spammers."

- How?
- Who are the spammers?

Critique

"Our analysis confirms that today's spamming business operates at a frightening scale without requiring truly sophisticated mechanisms to conquer the hurdles put in place by the anti-spam industry. Thus, to the detriment of productivity worldwide, the filtering arms race continues."

- Weak conclusion

Question for you

You have just downloaded and executed binaries that were propagated by the Storm Botnet. You are now a worker bot.

Soon after you are blacklisted from forums and wikis which you have never visit.

How would you feel?

What are the ways to counter this problem?