Joshua White
CS644
Professor: Dr. Jeanna Matthews

Short Paper Review of:
The nocebo effect on the web: an analysis of fake anti-virus distribution

Citation:

Moheeb Abu Rajab, Lucas Ballard, Panayiotis Mavrommatis, Niels Provos, and Xin Zhao. 2010. The nocebo effect on the web: an analysis of fake anti-virus distribution. In *Proceedings of the 3rd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more* (LEET'10). USENIX Association, Berkeley, CA, USA, 3-3.

Author(s) Affiliation(s):

- Google Inc.

Claims:

- Analysis of 240 million web pages collected by googles malware infrastucture
  - over a 13 month period
  - 11,000 domains involved in fake AV distribution
- They show that the Fake AV threat is rising
  - both in total and in in comparison to other forms of malware
- Their investigation reviels that fake AVs have several characteristics from other forms of web-based malware
  - They then show how these characteristics have changed over time

Likes:

- These attacks depend on the users being gullible.
- Any social engineering based attacks are very interesting.
- This paper dictates yet another reason we need a way to detect phishing sites.
- Very simple concept for a paper, a deep and insightful analysis.
- Interesting that the domain to AS ratio was ~20:1
- Interesting that the largest proportion of hosting/exploited Fake AV sites/end-users was in the USA

Dislikes:

- Typical google paper, they have a large collection infrastructure but they do not explain how their malware collection/detection infrastructure works.

Repeat / Add to Work?

- Good paper, though the authors should have included details about the collection infrastructure.

- This is the type of paper that I would like to reproduce in detail, with the exception of where the links come from. I would like to do a similar study using the URL's collected from twitter.