Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 7, July 2013, pg.406 – 412

RESEARCH ARTICLE

Identifying Under Attack Hateful Email

M. Ramu[1], B. Triveni[2], L. Srinivasa Rao[3]

[1]Assistant Professor, Department of Computer Science and Engineering,
Teegala Krishna Reddy Engineering College, JNTU Hyderabad, Andhra Pradesh, India
[2]Assistant Professor, Department of Computer Science and Engineering,
Teegala Krishna Reddy Engineering College, JNTU Hyderabad, Andhra Pradesh, India
[3]Scientist, Department of Information Systems, Defence Research and Development Laboratory (DRDL),
Ministry of Defence, Hyderabad, Andhra Pradesh, India

[1] ramumooducse@gmail.com; [2] triveni.banavatu@gmail.com

Abstract— unsolicited email is not only a nuisance but can be potentially dangerous. Methods to filter it out work fairly well with conventional unsolicited commercial email or email soliciting personal information but they don't work as well with under attack hateful email (AHE) that facilitates computer network exploitation. Current detection algorithms work well for spam and phishing because it's easy to detect mass-generated email sent to millions of addresses nit's possible to gather emails with similar characteristics and message content to probabilistically identify them. AHE, on the other hand, targets single users or small groups in low volumes. It's tailored specifically to the goal recipient and engineered to appear legitimate and trustworthy. If we rely on current conventional detection methods, AHE goes undetected.

Key Terms: - filtering; emails; hateful attacks; records

Full Text: http://www.ijcsmc.com/docs/papers/July2013/V2I7201388.pdf