

An Practical Investigation of Phishing Blacklists

Vivek Prasad¹ and Rohit Vishwakarma²

Assistant Professor, BSC IT, Suman Education Society's LN College, Borivali East, Mumbai, India¹

Student, BSC IT, Suman Education Society's LN College, Borivali East, Mumbai, India²

Abstract: *In this research, we investigate the efficacy of phishing blacklists. We utilised 191 fresh phishes that were less than 30 minutes old to do two tests on eight anti-phishing toolbars. We discovered that 63% of the phishing efforts in our sample lasted less than two hours. Blacklists were originally useless in safeguarding users, since most of them detected fewer than 20% of phish at hour zero. We also discovered that blacklists were updated at different rates and had varying coverage, with 47% - 83% of phish appearing on blacklists 12 hours after the original test. We discovered that two programmes that used heuristics in addition to blacklists captured substantially more phish from the start than those that merely used blacklists. However, phish spotted by heuristics took a long time to emerge on blacklists. Finally, we ran the toolbars against a database of 15,345 authentic websites. URLs for false positives and found no evidence of mislabelling for blacklists or heuristics. We show our findings and explain how anti-phishing solutions might be improved.*

Keywords: Phishing, Blacklists, Investigation, Evidence, research.

REFERENCES

- [1]. S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair. A comparison of machine learning techniques for phishing detection. In eCrime '07: Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit, pages 60–69, New York, NY, USA, 2007. ACM.
- [2]. Andy Patrizio. Symantec readies phishing protection software, august 7, 2006. visited jan 1, 2009. <http://www.smallbusinesscomputing.com/news/article.php/3624991>.
- [3]. AOL Press Release. Its 3 a.m. are you checking your email again? july 30, 2008. visited jan 1, 2009. <http://corp.aol.com/press-releases/2008/07/it-s-3-am-are-you-checking-your-email-again>.
- [4]. Apple Inc. . Visited jan 1, 2009. <http://www.apple.com/safari/features.html#security>.
- [5]. ASSOCIATED BANK-CORP v. EARTHLINK, INC. Memorandum and order, 05-c-0233-s. http://www.iplawobserver.com/cases/2005-09-14_Associated_Banc_Corp_CDA_Section_230.pdf.