Accurate Spear Phishing Campaign Attribution and Early Detection

Title	Accurate Spear Phishing Campaign Attribution and Early Detection
Publication Type	Conference Paper
Year of Publication	2016
Authors	Han, YuFei, Shen, Yun
Conference Name	Proceedings of the 31st Annual ACM Symposium on Applied Computing
Publisher	ACM
Conference Location	New York, NY, USA
ISBN Number	978-1-4503-3739-7
Keywords	attribution, composability, Human Behavior, Metrics, Pervasive computing, phishing, phishing attack, pubcrawl, semi-supervised learning, spear phishing emails

Abstract

There is growing evidence that spear phishing campaigns are increasingly pervasive, sophisticated, and remain the starting points of more advanced attacks. Current campaign identification and attribution process heavily relies on manual efforts and is inefficient in gathering intelligence in a timely manner. It is ideal that we can automatically attribute spear phishing emails to known campaigns and achieve early detection of new campaigns using limited labelled emails as the seeds. In this paper, we introduce four categories of email profiling features that capture various characteristics of spear phishing emails. Building on these features, we implement and evaluate an affinity graph based semi-supervised learning model for campaign attribution and detection. We demonstrate that our system, using only 25 labelled emails, achieves 0.9 F1 score with a 0.01 false positive rate in known campaign attribution, and is able to detect previously unknown spear phishing campaigns, achieving 100% 'darkmoon', over 97% of 'samkams' and 91% of 'bisrala' campaign detection using 246 labelled emails in our experiments.

URL	http://doi.acm.org/10.1145/2851613.2851801
DOI	10.1145/2851613.2851801

Citation Key han_accurate_2016

attribution composability Human behavior Metrics pervasive computing Phishing phishing attack pubcrawl semi-supervised learning spear phishing emails