Accepted Manuscript

Title: Panning for gold: automatically analysing online social engineering attack surfaces

Author: Matthew Edwards, Robert Larson, Benjamin Green, Awais Rashid, Alistair Baron

PII: S0167-4048(16)30184-5
DOI: http://dx.doi.org/doi: 10.1016/j.cose.2016.12.013
Reference: COSE 1085

To appear in: *Computers & Security*

Please cite this article as: Matthew Edwards, Robert Larson, Benjamin Green, Awais Rashid, Alistair Baron, Panning for gold: automatically analysing online social engineering attack surfaces, *Computers & Security* (2017), http://dx.doi.org/doi: 10.1016/j.cose.2016.12.013.

Panning for Gold: Automatically Analysing Online Social Engineering Attack Surfaces

Matthew Edwards*, Robert Larson, Benjamin Green, Awais Rashid, Alistair Baron*

Security Lancaster, School of Computing and Communications, Lancaster University, Lancaster, LA1 4WA, United Kingdom

*Corresponding authors

Email addresses: m.edwards7@lancaster.ac.uk (Matthew Edwards), r.larson@lancaster.ac.uk (Robert Larson), b.green2@lancaster.ac.uk (Benjamin Green), a.rashid@lancaster.ac.uk (Awais Rashid), a.baron@lancaster.ac.uk (Alistair Baron)

Abstract

The process of social engineering targets people rather than IT infrastructure. Attackers use deceptive ploys to create compelling behavioural and cosmetic hooks, which in turn lead a target to disclose sensitive information or to interact with a malicious payload. The creation of such hooks requires background information on targets. Individuals are increasingly releasing information about themselves online, particularly on social networks. Though existing research has demonstrated the social engineering risks posed by such open source intelligence, this has been accomplished either through resource-intensive manual analysis or via interactive information harvesting techniques. As manual analysis of large-scale online information is impractical, and interactive methods risk alerting the target, alternatives are desirable.

In this paper, we demonstrate that key information pertinent to social engineering attacks on organisations can be passively harvested on a large-scale in an automated fashion. We address two key problems. We demonstrate that it is possible to automatically identify employees of an organisation using only information which is visible to a remote attacker as a member of the public. Secondly, we show that, once identified, employee profiles can be linked across multiple online social networks to harvest additional information pertinent to successful social engineering attacks. We further demonstrate our approach through analysis of the *social engineering attack surface* of real critical infrastructure organisations. Based on our analysis we propose a set of countermeasures including an automated social engineering vulnerability scanner that organisations can use to analyse their exposure to potential social engineering attacks arising from open source intelligence.