Title: A survey of similarities in banking malware behaviours

Author: Paul Black, Iqbal Gondal, Robert Layton

PII: S0167-4048(17)30202-X
DOI: https://doi.org/doi:10.1016/j.cose.2017.09.013
Reference: COSE 1209

To appear in: *Computers & Security*

Received date: 30-8-2016
Revised date: 25-8-2017
Accepted date: 21-9-2017

A Survey of Similarities in Banking Malware Behaviours

Paul Black*, Iqbal Gondal[†], Robert Layton[‡]

Internet Commerce Security Lab, Federation University

Email: *paulblack@students.federation.edu.au, [†]iqbal.gondal@federation.edu.au, [‡]robertlayton@gmail.com

Paul Black is studying a PhD in Information Security at the Internet Commerce Security Lab (ICSL) at Federation University. His PhD topic is Techniques for the Reverse Engineering of Banking Malware. Paul has a Masters of Computing, his research topic was the reversing of Zeus malware. Paul started his career as a programmer in 1981 and has worked in banking, defence, law enforcement and malware analysis.

Dr. Iqbal Gondal is a leading researcher in the area of condition monitoring, sensor information processing, wireless communication and cyber security. Currently he is Director of Internet Commerce Security Lab (ICSL), Federation University Australia. ICSL conducts research in the application of advance analytics techniques for cybersecurity and condition monitoring and provides innovative Cybersecurity solutions to the industry. In the past, he was director of ICT strategy for the faculty of IT in Monash. He has served in the capacity of Director of Postgraduate studies for six years, member faculty board and member of Monash academic board. He is Fellow of Engineers Australia.

Dr. Robert Layton is a Data Scientist working with text problems in a number of domains. His research focuses on the methods used to build cybercrime attacks and the analysis of the outcomes. He is an Honorary Research Fellow at Federation University Australia and the inaugural Federation University Young Alumni of the Year in 2014.

Abstract—**Banking malware are a class of information stealing malicious software that target the financial industry. Banking malware families have become persistent with new versions being released by the original authors or by others using leaked source code. This paper draws together a fragmented and industry based literature to provide a coherent description of major banking malware families, their variants, relationships and source code leakages. The concept of malware behaviour is well established in the research**