Accepted Manuscript

Title: Automated poisoning attacks and defenses in malware detection systems: an adversarial machine learning approach

Author: Sen Chen, Minhui Xue, Lingling Fan, Shuang Hao, Lihua Xu, Haojin Zhu, Bo Li

PII: S0167-4048(17)30244-4
DOI: https://doi.org/10.1016/j.cose.2017.11.007
Reference: COSE 1234

To appear in: *Computers & Security*

Received date: 17-4-2017
Revised date: 31-10-2017
Accepted date: 12-11-2017

Please cite this article as: Sen Chen, Minhui Xue, Lingling Fan, Shuang Hao, Lihua Xu, Haojin Zhu, Bo Li, Automated poisoning attacks and defenses in malware detection systems: an adversarial machine learning approach, *Computers & Security* (2017), https://doi.org/10.1016/j.cose.2017.11.007.

Automated Poisoning Attacks and Defenses in Malware Detection Systems: An Adversarial Machine Learning Approach

Sen Chen[a,b], Minhui Xue[c,d], Lingling Fan[a,b], Shuang Hao[e], Lihua Xu[a,]*, Haojin Zhu[d], Bo Li[f]

[a]*East China Normal University, Shanghai, China*

[b]*Nanyang Technological University, Singapore*

[c]*New York University Shanghai, Shanghai, China*

[d]*Shanghai Jiao Tong University, Shanghai, China*

[e]*University of Texas at Dallas, USA*

[f]*University of California, Berkeley, USA*

Biography

Sen Chen is pursuing his Ph.D. degree at the School of Computer Science and Software Engineering of East China Normal University, focusing primarily on areas of smartphone security, Android malware, vulnerability and program analysis. He has received the MobiCom 2016 Travel Grant Award. He is currently serving as a visiting scholar in Cyber Security Lab at Nanyang Technological University. He is currently advised by Professor Lihua Xu (ECNU) and Yang Liu (NTU).

Minhui Xue is pursuing his Ph.D. degree at the School of Computer Science and Software Engineering of East China Normal University. He is also serving as a visiting scholar at the Courant Institute of Mathematical Sciences and Tandon School of Engineering at New York University, as well as a research assistant at New York University Shanghai, advised by

*Corresponding author. Email address: lhxu@cs.ecnu.edu.cn.

We would like to thank Pwnzen Infotech Inc. for providing us with a copy of mobile malware to conduct the study, especially the Pwnzen Infotech Inc. co-founder Zhushou Tang for exchanging helpful industry experience. This work was supported in part by the National Natural Science Foundation of China, under Grant 61502170, 61272444, 61411146001, U1401253, and U1405251, in part by the Science and Technology Commission of Shanghai Municipality under Grant 13ZR1413000.

Email addresses: ecnuchensen@gmail.com (Sen Chen), minhuixue@nyu.edu (Minhui Xue), ecnujanefan@gmail.com (Lingling Fan), shao@utdallas.edu (Shuang Hao), lhxu@cs.ecnu.edu.cn (Lihua Xu), zhuhaojin@gmail.com (Haojin Zhu), lxbosky@gmail.com (Bo Li)