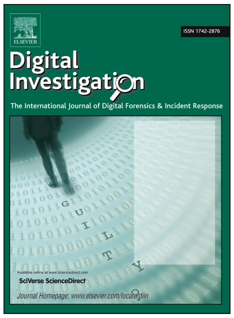

Dismantling OpenPuff PDF steganography

Thomas Sloan, Julio Hernandez-Castro

PII: S1742-2876(17)30328-6

DOI: 10.1016/j.diin.2018.03.003

Reference: DIIN 750

To appear in: *Digital Investigation*

Received Date: 9 October 2017

Revised Date: 5 February 2018

Accepted Date: 12 March 2018

Please cite this article as: Sloan T, Hernandez-Castro J, Dismantling OpenPuff PDF steganography, *Digital Investigation* (2018), doi: 10.1016/j.diin.2018.03.003.

Dismantling OpenPuff PDF Steganography

Thomas Sloan*, Julio Hernandez-Castro

University of Kent

School of Computing

Canterbury, CT2 7NF

Abstract

We present in this paper a steganalytic attack against the PDF component of the popular OpenPuff tool. We show that our findings allow us to accurately detect the presence of OpenPuff steganography over the PDF format with the use of a simple script. OpenPuff is a prominent multi-format and semi-open-source stego-system with a large user base. Because of its popularity, we think our results could potentially have relevant security implications. The relative simplicity of our attack, paired with its high accuracy and the existence of previous steganalytic findings against this software warrants major concerns over the real security offered by this steganography tool.

Keywords: Steganography, Steganalysis, OpenPuff, Privacy

1. Introduction

Steganography is the process of hiding information in plain sight. This can be used to carry out secret communications or avoid suspicion over possession of information. It is important to emphasise that the objectives of steganography are very different to those of cryptography. The latter provides confidentiality but does not disguise the existence of secret data, which is obvious to any observer and can even be automatically detected due to the high entropy of encrypted data. Steganography, however, aims to avoid detection under all circumstances, even when an active warden has

*Corresponding Author

Email addresses: `ts424@kent.ac.uk` (Thomas Sloan), `jch27@kent.ac.uk` (Julio Hernandez-Castro)