Accepted Manuscript

Title: R-locker: thwarting ransomware action through a honeyfile-based approach

Author: J.A. Gómez-Hernández, L. Álvarez-González, P. García-Teodoro

PII: S0167-4048(17)30256-0
DOI: https://doi.org/10.1016/j.cose.2017.11.019
Reference: COSE 1246

To appear in: *Computers & Security*

Received date: 14-7-2017
Revised date: 16-11-2017
Accepted date: 28-11-2017

Please cite this article as: J.A. Gómez-Hernández, L. Álvarez-González, P. García-Teodoro, R-locker: thwarting ransomware action through a honeyfile-based approach, *Computers & Security* (2017), https://doi.org/10.1016/j.cose.2017.11.019.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

R-Locker: Thwarting Ransomware Action through a Honeyfile-based Approach

J.A. Gómez-Hernández, L. Álvarez-González, P. García-Teodoro

Network Engineering & Security Group (https://nesg.ugr.es)

CITIC - University of Granada

Email: jagomez@ugr.es, luciaalvarez@correo.ugr.es, pgteodor@ugr.es

José Antonio Gómez-Hernández is an Assistant Professor at the Departament of "Languages and Computer Systems" of the University of Granada, and member of the research group "Network Security & Engineering Group (NESG)" and "UGR Cyber Security Group (UCyS)" of the same university. His professional interest is related with operating system security and computer forensics.

Lucía Álvarez-González is graduated in Telecommunication Technologies Engineering by the University of Granada, and is currently a student of the Master in Telecommunication Engineering of this university. Her interest is focused on cybersecurity and communications.

Pedro García-Teodoro is a Full Professor of the Department of "Signal Theory, Telematics and Communications" of the University of Granada, and head of the research groups "Network Security & Engineering Group (NESG)" and "UGR Cyber Security Group (UCyS)" of this university. His current professional interest is in the field of computer and network security, especially focused on intrusion and anomaly-based detection.

Abstract

Ransomware has become a pandemic nowadays. Although some proposals exist to fight against this increasing type of extorsion, most of them are prevention like and rely on the assumption that early detection is not so effective once the victim is infected. This paper presents a novel approach intended not just to early detect ransomware but to completly thwart its action. For that, a set of *honeyfiles* are deployed around the target environment in order to catch the ransomware. Instead of being normal archives, honeyfiles are FIFO like, so that the ransomware is blocked once it starts reading the file. In addition to frustrate its action, our honeyfile solution is able to automatically launch countermeasures to solve the infection. Moreover, as it does not require previous training or knowledge, the approach allows fighting against unknown, zero-day ransomware related attacks. As a proof of concept, we have developed the approach for Linux

Accepted Manuscript

Download English Version:

https://daneshyari.com/en/article/6884080

Download Persian Version:

https://daneshyari.com/article/6884080

Daneshyari.com