Tạp chí KHOA HỌC & CÔNG NGHỆ - Đại học Công nghiệp Hà Nội số 38A (2/2017):103-107

# XÂY DỰNG TẬP LUẬT SNORT ĐỂ PHÁT HIỆN VÀ NGĂN CHẶN SỰ THỰC THI CỦA MÃ ĐỘC TỐNG TIỀN LOCKY VÀ CRYPTXXX

## CREATE SNORT RULES IN ORDER TO DETECT AND PREVENT ENFOERCING PROCESS OF LOCKY AND CRYPTXXX RANSOMWAVE

**Nguyễn Đăng Tiến**[1*]

[1]Trường Đại học Kỹ thuật - Hậu cần CAND

[*]E-mail: dangtient36@gmail.com

Ngày nhận bài: 30/11/2016

Ngày nhận bài sửa sau phản biện: 23/02/2017

Ngày chấp nhận đăng: 28/02/2017

**TÓM TẮT** Hiện nay, Locky và CryptXXX là hai họ phần mềm mã độc tống tiền phổ biến và gây thiệt hại lớn tới dữ liệu và tài chính của nhiều tổ chức, cá nhân. Các phương pháp phòng tránh đã được đưa ra, tập trung chủ yếu vào việc nâng cao hiểu biết, ý thức tự bảo vệ của mỗi người dùng trên Internet hay loại bỏ các lỗ hổng phần mềm để tránh bị khai thác. Bài báo phân tích cơ chế lây nhiễm, mã hóa và đặc điểm truyền thông của Locky và CryptXXX, từ đó xây dựng, đề xuất ứng dụng các tập luật vào hệ thống Snort để phòng chống lây nhiễm cũng như ngăn chặn quá trình thực thi bình thường của chúng khi lây nhiễm vào máy tính. Sử dụng Snort là một biện pháp độc đáo, khả thi với tỉ lệ phát hiện nhầm thấp.

***Từ khóa:*** *Ransomware, Locky, CryptXXX, luật Snort.*

**ABSTRACT** Currently, Locky and CryptXXX are two popular Ransomware Families. They cause major damage to the finance and data of many organizations and individuals. The methods of prevention were brought out, focused mainly on enhancing knowledge and self-protection awareness of each Internet user or removing software gaps in order to avoid being exploited. This paper analyze the mechanisms of infection and encoding, and communication characteristics of Locky and CryptXXX. Since then, will propose and create the application of rules to Snort system in order to prevent infection as well as their normal enforcing process when accessing a computer. Using Snort is very exciting and feasible with low rates of wrong detection.

***Keywords:*** *Ransomware, Locky, CryptXXX, Snort Rules.*