Tạp chí KHOA HỌC & CÔNG NGHỆ - Đại học Công nghiệp Hà Nội - Số 40 (6/2017): **3-7**

# PHÂN TÍCH PETYA - MỘT BIẾN THỂ MỚI CỦA PHẦN MỀM MÃ ĐỘC TỐNG TIỀN

## PETYA - A NEW VARIATION OF RANSOMWARE

***Nguyễn Đăng Tiến***
*Trường Đại học Kỹ thuật - Hậu cần CAND*

**TÓM TẮT**

Petya là một biến thể mã độc tống tiền mới được ghi nhận vào ngày 27/6/2017 khi tấn công và làm tê liệt các hệ thống thông tin tại Ukraina. Mặc dù được xem là một mã độc tống tiền, tuy nhiên Petya lại có những đặc điểm khác biệt so các họ mã độc tống tiền khác. Trong bài báo này, tác giả trình bày về mã độc Petya, tập trung phân tích về cơ chế lây nhiễm, mã hóa của chúng. Bên cạnh đó là phân tích những điểm khác biệt của Petya so với các loại mã độc tống tiền thông thường. Đồng thời cũng đưa ra một số biện pháp để phát hiện và ngăn chặn sự lây nhiễm, bảo vệ máy tính và hệ thống thông tin trước mối nguy hiểm này.

***Từ khóa:*** *Mã độc tống tiền, Petya, NotPetya, MBR*

**ABSTRACT**

Petya is a variation of new ransomware detected on June 27, 2017 when it attacks and cripples information systems in Ukraine. Although considered as a ransomware, Petya has many characteristics which are different from the ones of other ransomwares. In this article, I will present about Petya and focus on analyzing their mechanism of infection and encoding. In addition, I will also analyze the differences of Petya when it is compared to the common ransomware. Finally, I will recommend some solutions to detect and prevent infection, protect computers and information systems against this ransomware.

***Keywords:*** *Ransomware, Petya, NotPeyta, MBR.*

---

*Email: ndtient36@gmail.com*
*Ngày nhận bài: 30/06/2017*
*Ngày nhận bài sửa sau phản biện: 06/07/2017*
*Ngày chấp nhận đăng: 07/07/2017*