

NGHIÊN CỨU MÃ ĐỘC MIRAI - CÔNG CỤ TẠO BOTNET MỚI ĐỂ TẤN CÔNG TỪ CHỐI DỊCH VỤ SỬ DỤNG CÁC THIẾT BỊ INTERNET OF THINGS

MIRAI MALWARE - NEW BOTNET TOOL TO ATTACK TECHNIQUE FOR DENIAL OF SERVICE USING INTERNET OF THINGS

Nguyễn Đăng Tiến

Trường Đại học Kỹ thuật - Hậu cần CAND

TÓM TẮT

Internet of Things (IoT) đang là một xu thế phát triển mạnh trên toàn cầu. Các thiết bị IoT xuất hiện phổ biến và ứng dụng vào hầu hết các lĩnh vực của đời sống, mang lại nhiều lợi ích cho xã hội. Đi kèm với đó là các nguy cơ bị khai thác, đánh cắp dữ liệu hay bị sử dụng cho mục đích trái phép do nhận thức chưa đầy đủ và vấn đề bảo mật còn yếu. Năm 2016, thế giới ghi nhận kỹ thuật tấn công từ chối dịch vụ mới sử dụng mã độc Mirai để điều khiển một mạng BotNet gồm các thiết bị IoT tấn công vào các công ty lớn của Mỹ và Pháp, với băng thông kỷ lục đến 1,5Tbps. Việt Nam là nước có tỉ lệ là nơi xuất phát của các cuộc tấn công sử dụng mã độc Mirai cao nhất trên thế giới. Trong bài báo này, tác giả giới thiệu về một kỹ thuật tấn công từ chối dịch vụ mới sử dụng các thiết bị IoT, mô hình hoạt động của mạng BotNet Mirai và phân tích mã nguồn, kỹ thuật lây nhiễm và thực thi của chúng. Phần cuối, đề xuất các biện pháp cơ bản để người dùng bảo vệ thiết bị của mình trước sự lây nhiễm của mã độc này.

Từ khóa: *Mirai, DDOS, Internet kết nối vạn vật, BotNet, mã độc.*

ABSTRACT

Internet of Things (IoT) is a developing trend all over the world. IoT devices become more popular and they are applied to most fields of life, bringing many benefits to society. That is accompanied by the risk of being exploited, stolen or used data for unauthorized purposes due to users' insufficient awareness and weak security. In 2016, the world recognized a new attack technique for denial of service using Mirai malware to control the BotNet network including IoT devices that attacked major US and French companies, with record bandwidth to 1.5Tbps. Vietnam is the leading country in the world with the highest number of attacks of Mirai malware. In this article, I introduce a attack technique for denial of service using IoT devices, the operation model of the Boti Botnet network, and analysis of their source code, propagation and execution techniques. Lastly, I offer basic measures for users to protect their devices against the infection of this malware.

Keyword: *Mirai, DDOS, Internet of Things, BotNet, Malware.*

Email: dangtient36@gmail.com

Ngày nhận bài: 01/08/2017

Ngày nhận bài sửa sau phân biện: 04/09/2017

Ngày chấp nhận đăng: 16/10/2017

TÓM TẮT

Đối với các khu vực có mật độ phụ tải thấp, việc lựa chọn nguồn cung cấp giữa nguồn điện lưới và nguồn điện phân tán (DG) luôn là bài toán được đặt ra bởi chỉ tiêu kinh tế. Hiện nay, do suất đầu tư các nguồn DG ở nước ta còn khá cao so với nguồn năng lượng truyền thống, nên đối với từng khu vực cụ thể sẽ cho kết quả lựa chọn là rất khác nhau. Đã có nhiều phương pháp để giải quyết bài toán này nhưng chưa có lời giải cụ thể đối với từng khu vực đặc trưng và đặc biệt là khi xét đến đặc tính công suất của DG. Trong bài báo này, nhóm tác giả sẽ áp dụng phương pháp chi phí vòng đời (LCC) để giải quyết bài toán nêu trên, áp dụng cụ thể cho khu vực xa lưới ở huyện Tân Lạc, tỉnh Hòa Bình. Nghiên cứu này có thể áp dụng tại các địa phương có đặc điểm tương tự, nhằm giải quyết bài toán cân bằng điện năng của Việt Nam một cách bền vững.

Từ khóa: Mật độ phụ tải, nguồn điện phân tán, LCC, mở rộng lưới điện.

ABSTRACT

For areas with low load density, the choice of power supply between grid and renewable energy is always the problem set by the economic indicator. Currently, because the investment in distributed generations in our country is relatively high compared to traditional energy sources, so for each specific area will result in very different choices. There are many methods to solve this problem but there is no specific solution for each specific area, and especially considering the characteristics of distributed generations. In this paper, we will apply the LCC method to solve the above problem, specifically for the remote area in Tan Lac district, Hoa Binh province. This study may be applied in similarly-sampled localities to calculate the electric energy balance of the low load density region.

Keywords: Load density, distributed generation, LCC, grid extension.

Email: tuanna@hau.edu.vn

Ngày nhận bài: 20/01/2017

Ngày nhận bài sửa sau phản biện: 09/10/2017

Ngày chấp nhận đăng: 16/10/2017