C15 BẮT GIỮ MỘT ĐỐI TƯỢNG TẤN CÔNG DDOS

Đơn vị Phòng chống tội phạm công nghệ cao C15 - Bộ công an vừa tiến hành bắt giữ một số đối tượng liên quan đến tội phạm công nghệ cao: tấn công từ chối dịch vụ (DDoS) có chủ đích vào hệ thống máy chủ của công ty Nhân Hòa (Hà Nội). Ông Trần Văn H

Đơn vị Phòng chống tội phạm công nghệ cao C15 - Bộ công an vừa tiến hành bắt giữ một số đối tượng liên quan đến tội phạm công nghệ cao: tấn công từ chối dịch vụ (DDoS) có chủ đích vào hệ thống máy chủ của công ty Nhân Hòa (Hà Nội). Ông Trần Văn Hòa - trưởng đơn vị Phòng chống tội phạm công nghệ cao C15 (Bộ Công an) khẳng định, trong buổi sáng hôm qua - 31/7/2006 - C15 đã tiến hành bắt giữ một đối tượng ở Bắc Ninh, sau khi có bằng chứng xác đáng về việc người này cùng một số đối tượng khác liên tục tấn công từ chối dịch vụ (DDoS) với ý đồ xấu vào hệ thống máy chủ của công ty Nhân Hòa - (Công ty cung cấp dịch vụ Hosting và Domain có trụ sở tại Hà Nội). Vụ việc nói trên đã được C15 âm thầm tiến hành điều tra hơn một tháng nay. Cho đến hiện tại, dù đã có những bằng chứng xác đáng, C15 vẫn chưa công bố tên tuổi và các hình thức xử lý với đối tượng bị bắt, song họ khẳng định sẽ đưa ra các thông tin sau khi hoàn tất các thủ tục cần thiết.

Tấn công DDOS bằng xflash có sức phá hoại không thể chống đỡ!

Ông Vũ Đức Trung - (giám đốc công ty Nhân Hòa - người viết lá đơn nhờ C15 vào cuộc điều tra) cho biết: Cách đây khoảng 4 tháng, các máy chủ của công ty ông bị tấn công từ chối dịch vụ liên tiếp một cách đáng ngờ. "Việc tấn công DDoS dữ dội vào các website ngẫu nhiên của khách hàng đặt trên server (máy chủ) của chúng tôi khiến toàn bộ hệ thống bị quá tải và làm chúng tôi ngày càng mất dần khách hàng. Việc này ảnh hưởng nghiêm trọng đến số lượng khách hàng, chất lượng phục vụ và uy tín của công ty" - Ông Trung nói. Sau khi theo dõi và "chịu đựng" một thời gian dài, ông Trung cho rằng công ty của mình đang bị tấn công một cách có chủ đích: "Rất có thể là một sự cạnh tranh không lành mạnh từ một công ty kinh doanh dịch vụ tương tự". Từ đó ông Trung bắt đầu theo dõi - ghi lại các diễn biến của từng đợt tấn công và gửi file log sang trung tâm An ninh mạng BKIS - ĐH Bách Khoa HN nhờ đơn vị này giúp đỡ. "Trong quyền hạn của mình, BKIS chỉ có thể tìm ra các đầu mối, các thông tin liên quan có giá trị, sau đó chúng tôi khuyên Nhân Hòa hãy nộp đơn cho C15 - Đơn vị này mới có đủ thẩm quyền điều tra." - Ông Nguyễn Tử Quảng - giám đốc trung tâm BKIS cho biết. Với sự vào cuộc đầy quyết tâm của C15 cùng với sự phối hợp của BKIS, vụ việc đã được đưa ra ánh sáng. Theo ông Quảng, ở Việt Nam hiện tại có hai hình thức tấn công từ chối dịch vụ khiến nhiều người đau đầu: Sử dụng mạng Botnet và tấn công Xflash. Trước đây C15 cũng từng xử lý một vụ việc điển hình, bắt giữ đối tượng Nguyễn

Thành Công (DantruongX) vì đã tấn công từ chối dịch vụ gây thiệt hại vào hệ thống website TMĐT của công ty VietCo. Khi đó DantruongX sử dụng mạng Botnet để tấn công, còn hình thái mà nhóm DDoSer lần này sử dụng tấn công Nhân Hòa là XFlash. Thực ra thì cả hai hình thái DDoS này đều rất ác ý và có sức hủy diệt lớn đối với các hệ thống thông tin. "Không chỉ VietCo và Nhân Hòa, theo tôi được biết thì hầu hết các hệ thống thông tin và thương mại điện tử ở Việt Nam đều đang bị DDoS quấy rối. Những động thái xử lý răn đe của pháp luật vào lúc này theo tôi là rất cần thiết!" - Ông Quảng kết luận. Thế Phong