HEZBOLLAH ĐANG... TẤN CÔNG INTERNET

Cửa sổ pop up của lực lượng du kích Hezbolla xổ ra từ đủ mọi website trên mạng, với nội dung chiêu binh, kêu gọi đóng góp và tuyên truyền. Một mạng cáp ở ngoại ô Virginia và máy chủ hosting ở Delhi, Montreal, Brooklyn rồi New Jersey có điểm nào chung?

Cửa sổ pop up của lực lượng du kích Hezbolla xổ ra từ đủ mọi website trên mạng, với nội dung chiêu binh, kêu gọi đóng góp và tuyên truyền. Một mạng cáp ở ngoại ô Virginia và máy chủ hosting ở Delhi, Montreal, Brooklyn rồi New Jersey có điểm nào chung? Kể từ khi chiến sự nổ ra ở Libăng, các cổng liên lạc của họ đều đã bị lực lượng du kích Hezbollah tấn công hijack. Vũ khí mới

Một thông điệp được phát đi trên kênh truyền hình Al-Manar từ thủ lĩnh nhóm Hồi giáo Shiite tại Libăng. Nguồn: AFP

Các hacker trực thuộc lực lượng này đã lang thang sục sạo trên mạng Internet, săn lùng những website sơ hở để phát sóng các thông điệp của kênh truyền hình Al-Manar (bị phía Mỹ cấm), cũng như để liên lạc với thế giới bên ngoài. Trong chủ nghĩa khủng bố, chiến thuật này chẳng xa lạ gì, giống như một vũ hội hóa trang cổ xưa, các site Hezbolla nổi lên, bị hạ rồi lại "tái sinh" ở đâu đó trên không gian World Wide Web rộng lớn này. "Khi Israel xiết chặt thòng lọng vào cổ Hezbolla tại Libăng, những "nút" liên lạc này trở nên sống còn", Fred Burton, cựu quan chức chống khủng bố của Mỹ - nay về làm phó chủ tịch hãng bảo mật Stratfor cho biết. Internet đang trở thành một nguồn sống mới cho những lực lượng như Hezbollah trong công cuộc chiêu binh mãi mã, quyên tiền, tuyên truyền, liên lạc .... Vụ hijack mới đây nhằm vào một mạng cáp ở miền Nam Texas có thể coi là thí dụ điển hình cho sự xâm nhập của Hezbollah. Hãng cáp này có hợp đồng với một công ty "tập kết" tín hiệu vệ tinh ở New York, theo đó, các luồng dữ liệu truyền về sẽ được "tiếp sóng" đến khách hàng ở khắp nơi trên thế giới, bao gồm cả Libăng. Những kẻ "câu trộm" Tuy nhiên, ít lâu sau khi chiến sự bùng nổ, hệ thống của hãng này ... mọc thêm một "kết nối" trái phép. Lẽ tất nhiên, kênh kết nối này là do Hezbollah mở ra. Kênh truyền hình Al-Manar - được coi là phát ngôn viên của Hezbollah và bị phía Mỹ quy vào hàng khủng bố - đã kết nối với địa chỉ IP của hãng cáp nói trên. Nói thế này để độc giả có thể hình dung đơn giản hơn: Hãng cáp Texas có một đường dây điện thoại (tức là IP) và Hezbollah đã "câu trộm" đường dây này để truyền tín hiệu. Sau khi "câu trộm", Hezbollah bắt đầu "phát ngôn" thông qua những email và blog mà họ tìm được bên trong địa chỉ IP. Nếu vụ tấn công không bị phát hiện, địa chỉ IP có thể kết nối với một tên miền mới và bất cứ ai khi tìm kiếm từ khóa Al-Manar đều có thể mở vào site đó. Hezbollah sử dụng những site này để đăng tải các video tuyển tân binh và tài khoản ngân hàng nơi những

người ủng hộ có thể quyên góp, hỗ trợ. Mèo vờn chuột Tuy nhiên, vụ hijack này đã nhanh chóng bị tổ chức Nghiên cứu Internet khui ra. Tổ chức này đã lập tức thông báo cho hãng cáp Texas và nhà chức trách Mỹ, còn địa chỉ IP bị "câu" đã bị đóng cửa ngay sau đấy. Tuy nhiên, Aaron Weisburd, một chuyên gia lập trình của Nghiên cứ Internet cho rằng đóng cửa các website Hezbollah cũng giống như "con dao hai lưỡi". Là một cựu quan chức chống khủng bố của Mỹ, ông biết được giá trị của việc "duy trì" các site này, để cho các cơ quan tình báo có thể thu thập được bằng chứng pháp lý. "Xem họ nói những gì là một việc rất quan trọng", Weisburd nói, nhấn mạnh rằng Hezbollah còn có căn cứ tại Indonesia và khu vực ba biên giới (Brazil, Argentina, Paraguay) ở Nam Mỹ. Chịu khó theo dõi chặt sự hiện diện của Hezbollah trên mạng internet có thể giúp sớm kết thúc trò chơi mèo vờn chuột của lực lượng này với tình báo phương Tây. Mặc dù vậy, đóng cửa các site cũng giúp hạn chế các hoạt động tuyển mộ, tài chính và tuyên truyền của chúng. Cuộc chiến dài hơi Tháng 3/2006, đội quân săn lùng "khủng bố mạng" đã có thêm một vũ khí mới khi Cục dự trữ liên bang Mỹ tuyên bố bất cứ công ty Mỹ nào có quan hệ làm ăn với Al-Manar cũng sẽ bị trừng phạt. Quy định này có nghĩa là những chuyên gia tình nguyện của Nghiên cứu Internet có thể nhắc nhở các công ty hosting chần chừ, do dự hoặc không hợp tác rằng họ đang phải đối mặt với án phạt từ chính phủ. Trong trường hợp hãng cáp Texas. Chỉ vài tiếng sau khi cổng IP này bị đóng cửa, Hezbollah đã phản ứng nhanh chóng, "câu trộm" vào IP của một công ty Web-hosting của Ấn. "Chừng nào cuộc chiến còn tiếp diễn, những cổng thông tin kiểu này sẽ không bao giờ biến mất, vì Hezbollah buộc phải đưa thông điệp của họ ra toàn thế giới", Burton nói. Trọng Cầm