MÁY CHỦ DNS CỦA FPT BỊ TẤN CÔNG?

Từ vài ngày qua, nhiều thuê bao ADSL của FPT phản ánh hiện tượng khi truy cập vào hầu hết các địa chỉ website quốc tế có đuôi tên miền .org đều bị chuyển hướng (redirect) trình duyệt sang trang chủ của website www.myfamily.com. Theo thông tin thẩm định của một số chuyên

Từ vài ngày qua, nhiều thuê bao ADSL của FPT phản ánh hiện tượng khi truy cập vào hầu hết các địa chỉ website quốc tế có đuôi tên miền .org đều bị chuyển hướng (redirect) trình duyệt sang trang chủ của website www.myfamily.com. Theo thông tin thẩm định của một số chuyên gia an ninh mạng trả lời VietNamNet trong sáng Chủ nhật (21/5), bước đầu đã xác định được đây là lỗi phân giải tên miền ở máy chủ DNS dns2.fpt.vn của nhà cung cấp DV Internet (ISP) FPT. Máy chủ DNS này có nhiệm vụ phân giải tên miền cho các thuê bao ADSL.

Kết quả ping tới máy chủ dns2.fpt.vn trả về địa chỉ IP 210.245.0.10.

Để xác minh sự cố này, kỹ thuật viên đã thử truy cập vào các website có đuôi .org qua máy chủ DNS nói trên. Trước tiên, khi thực hiện lệnh ping dns2.fpt.vn, địa chỉ IP của máy chủ DNS này trả về là 210.245.0.10. Đặt địa chỉ này vào phần khai báo DNS Server của đường truyền VDC hay Viettel, khi truy cập vào phần lớn các website có đuôi .org đều có hiện tượng bị chuyển hướng truy cập sang trang chủ của myfamily.com, nhưng phần đầu của địa chỉ .org vẫn được giữ nguyên, chỉ thêm phần đường dẫn isapi.dll?c=home&htx=loginfrontmember phía sau.

Khi các thuê bao ADSL của VDC hay Viettel không dùng máy chủ DNS mặc định của ISP, chuyển sang dùng DNS Server 210.245.0.10 lập tức cũng gặp tình trạng bị chuyển tới myfamily.com khi truy cập vào các website có đuôi .org.

Cuối năm ngoái, cụ thể là ngày 14/11, các thuê bao ADSL của FPT trên diện rộng cũng từng gặp

phải tình trạng khi truy cập vào Google thì bị điều hướng trình duyệt sang một website bán hàng trực tuyến không tên tuổi. Lỗi này cũng được xác định nằm ở máy chủ phân giải tên miền (DNS Server) phục vụ các thuê bao ADSL của FPT. Đánh giá về nguyên nhân của sự cố này, một số chuyên gia cho biết không loại trừ khả năng máy chủ dns2.fpt.vn đã bị tấn công DNS server, sửa các DNS record trên cache của dns2.fpt.vn, để khi người dùng truy vấn vào các website này thì đều trả về website myfalimy.com. Nếu giả định trên là đúng thì đây là một lỗi bảo mật khá nghiêm trọng, vì kẻ tấn công DNS hijacking có thể điều hướng người truy cập tới một website bất kỳ do hắn tạo ra. Website đó có thể được cài sẵn các file flash có đuôi .exe hoặc những đoạn mã khai thác lỗi bảo mật mới của IE, để khi người dùng truy cập vào, lập tức máy tính của họ bị nhiễm virus, spyware, trojan... và bị chiếm quyền điều khiển. Lúc đó, các thông tin cá nhân trên máy tính như mã thẻ tín dụng, mật khẩu, dữ liệu... đều có thể bị lấy trộm khi bị kiểm soát từ xa.

Khi truy cập vào www.apache.org hay các website .org khác (xem ảnh mozdev.org, sans.org và worldbank.org) người dùng đều bị điều hướng trình duyệt tới trang chủ website myfamily.com.

Trong trường hợp này, myfamily.com là một website đã có từ năm 1998, chuyên về các dịch vụ web cá nhân dành cho nhóm gia đình, người thân, bạn bè, có số người truy cập tương đối động, đứng thứ hạng Alexa 2410. Theo nhận định sơ bộ, có vẻ động cơ của việc điều hướng trình duyệt tới myfamily.com là để quảng cáo. Chiều 21/5, phóng viên đã thử gọi đến số điện thoại hỗ trợ dịch vụ ADSL của FPT - 04–7601090 - vài lần để tìm hiểu nguyên nhân, nhưng số máy này bận liên tục không thể liên lạc được. Đến 1h30 sáng ngày 22/5, tình trạng truy cập vào các website có đuôi .org qua máy chủ dns2.fpt.vn vẫn chưa được khắc phục, người dùng web tiếp tục bị redirect tới trang myfamily.com. Minh Huy