# TIN TẶC LỢI DỤNG YAHOO RIGHT MEDIA PHÁT TÁN TROJAN

Hệ thố

Hệ thống mạng quảng cáo trực tuyến Right Media của Yahoo bất ngờ đã trở thành "đồng minh" của tin tặc, giúp chúng phát tán hàng triệu banner quảng cáo nhiễm Trojan trên hàng loạt website, trong đó có cả những tên tuổi như Photobucket và MySpace.

Một số hãng bảo mật đã nhận diện và xác định trojan được cấy trong banner quảng cáo của Yahoo Right Media là Trojan Downloader.VBS.Agent.n. Mục tiêu của nó là những PC chưa được cài đặt bản vá lỗi bảo mật Microsoft Data Access Components đã được Microsoft cho phát hành hồi tháng 2 vừa qua.

Hãng bảo mật ScanSafe cho biết banner quảng cáo "độc hại" nói trên bắt đầu xuất hiện thông qua mạng Right Media đầu tháng 8 vừa qua. Chỉ trong vòng có khoảng 3 tuần lễ nó đã được phát tán tới 12 triệu lần và xuất hiện trên 70 máy chủ quảng cáo khác nhau đan xen giữa các quảng cáo hợp pháp.

Nếu người dùng truy cập vào bất kỳ website nào có chứa banner quảng cáo "độc hại" nói trên sẽ ngay lập tức bị nhiễm một con trojan nguy hiểm. Tuy nhiên, trojan chỉ có thể tấn công những PC sử dụng phiên bản trình duyệt Internet Explorer chưa được cài đầy đủ bản vá lỗi cần thiết.

Hiện vẫn chưa thể thống kê được chính xác số lượng người dùng đã bị nhiễm con trojan này.

Phát biểu trước vấn đề này, người phát ngôn của Yahoo khẳng định hãng đã nhận diện được banner quảng cáo nguy hiểm và đã nhanh chóng loại bỏ. "Chúng tôi không thể kiểm soát được những gì diễn ra trên mạng Internet. Chúng tôi sẽ tiếp tục nỗ lực phát triển các công cụ bảo mật và cam kết sẽ tìm ra được giải pháp hiệu quả nhất để chống lại hình thức tấn công như thế này nhằm bảo vệ người dùng và nhà quảng cáo."

Tuy nhiên, người phát ngôn của Yahoo lại từ chối cho biết kế hoạch phòng chống một sự việc tương tự có thể xảy ra trong tương lai của Right Media. Đại diện của MySpace và Photobuck cũng chưa có bình luận chính thức nào về sự việc nói trên.

"Vô tình thành kẻ tiếp tay"

Right Media hiện đang là một trong những mạng quảng cáo trực tuyến mới nổi phát triển mạnh

nhất trên Internet với khoảng hơn 20.000 khách hàng là các hãng quảng cáo, cung cấp nội dụng và cung cấp dịch vụ mạng. Đây là một lợi thế song cũng là một điểm yếu chết người của Right Media. Sẽ rất khó có thể phân biệt được trong một số lượng khách hàng đông đến như thế ai là nhà quảng cáo hợp pháp và đâu là tin tặc muốn phát tán mã độc.

Right Media cũng thường xuyện tải về để kiểm tra xem những banner quảng cáo của khách hàng có "độc hại" hay không. Song tin tặc đã nhanh chóng tìm được biện pháp qua mặt cuộc kiểm tra này bằng cách lập trình một banner quảng cáo dạng flash có chức năng không bao giờ tấn công những hệ thống có dính dáng đến tên miền của Right Media. Ngoài cuộc kiểm tra đó Right Media không còn giải pháp bảo mật nào khác, tin tặc vì thế cứ vô tư mà phát tán mã độc.

"Không một ai tiến hành kiểm tra phân loại đâu là banner quảng cáo độc hại," ông Dan Nadir – phó chủ tịch phụ trách chiến lược sản phẩm của ScanSafe - khẳng định. "Vấn đề này sẽ còn tiếp tục xảy ra chừng nào chúng ta có giải pháp chứng thực người phát hành quảng cáo".

Kỹ thuật phát tán mã độc thông qua những quảng cáo trông như hoàn toàn hợp pháp không phải là một ý tưởng mới, đặc biệt đối với những người dùng MySpace. Tháng 7-2006, ước tính có khoảng 1 triệu người dùng website mạng xã hội này bị nhiễm một phần mềm quảng cáo (adware) cực kỳ nguy hiểm được "cấy" lên một quảng cáo trên trang.

Giới phân tích nhận định hình thức tấn công phát tán mã độc thông qua quảng cáo như thế vô cùng nguy hiểm và có tỉ lệ thành công rất cao. Nếu người dùng truy nhập một website độc hại bị nhiễm mã độc thì không sao. Đằng này họ truy cập website hợp pháp mà lại bị nhiễm mã độc.

H.Trang