BÙNG NỔ WEBSITE "PHISHING" TRÊN MẠNG WEB

Bạn tư

Bạn tưởng rằng bộ lọc phishing tích hợp mới bên trong hai trình duyệt IE7 và Firefox 2 sẽ bảo vệ được dữ liệu cá nhân của mình ư? Hãy nghĩ lại.

Số lượng website ra đời nhằm mục đích đào mỏ, lừa đảo và phishing đã gia tăng với tốc độ tên lửa hồi năm ngoái, còn số lượng nạn nhân của các phi vụ phishing cũng đông gần gấp đôi. Trong tháng 11/2006, Tổ chức chống Phishing Mỹ đã phát hiện được 37.500 website mới, tăng tới... 709% so với con số 4630 site của cùng kỳ năm trước.

Tháng 10 năm ngoái, cả Mozilla lẫn Microsoft đều phát hành những phiên bản trình duyệt mới nhất, với tính năng lập sổ đen các website phishing, rồi sử dụng danh sách này để chặn không cho người dùng truy cập vào những địa chỉ đó.

Để đáp lại, giới phisher lập tức dội bom thế giới mạng bằng hằng hà sa số những website ma, giả mạo mới, với tốc độ nhanh đến mức các bộ lọc khó lòng mà lập kịp danh sách hay xóa sổ.

Việc giới lừa đảo "đẻ" ra website mới dễ dàng đến mức báo động, cộng thêm hàng loạt chiến thuật lừa đảo kiểu mới, khiến cho giới bảo mật nhấp nhổm như phải lửa. Thậm chí, còn còn chua chát thừa nhận chính giới phisher mới là những kẻ trên cơ trong cuộc chiến này.

"Đến một giai đoạn nào đó, những công nghệ dựa dẫm quá nhiều vào sổ đen sẽ trở nên vô dụng", ông Zulfikar Ramzan, chuyên gia cấp cao của Nhóm Phản ứng Bảo mật Symantec cảnh báo.

Phishing như bóc kẹo

Nguồn: SecurityLabs

Tháng trước, các bộ công cụ "phishing" (cho phép bọn tội phạm lập ra những website giả mạo y như thật, có độ thuyết phục cực cao mà công sức bỏ ra lại hết sức khiêm tốn) bắt đầu được rao bán nhan nhản trên website "chợ đen".

Site giả mạo cóp hình ảnh và thiết kế layout từ website thật, thường là của ngân hàng hoặc tổ chức tài chính. Khi người dùng đăng nhập, các thông tin như tài khoản, mật khẩu sẽ được truyền trở lại website thật để quy trình log-in diễn ra bình thường. Người dùng không hề hay biết rằng bản sao của những dữ liệu nhạy cảm kia đã rơi vào tay bọn phisher.

Cùng với dòng dữ liệu ngồn ngộn đổ vào tay bọn tội phạm là những khoản lợi nhuận kếch xù. Hãng nghiên cứu Gartner ước tính có tới 3,5 triệu người Mỹ đã hớ hênh tiết lộ thông tin tối mật cho những kẻ lừa đảo trong năm 2006.

Con số này nhảy vọt tới 86% so với năm 2005 - và thiệt hại kinh tế mà họ phải gánh lên tới 2,8 tỷ USD. Một băng nhóm phishing có hạng tên là Rock Phish, thậm chí còn kiếm được hơn 100 triệu USD.

Theo các chuyên gia bảo mật, Rock Phish chính là thủ phạm nghĩ ra hàng loạt kỹ thuật mới, góp phần tạo ra sự bùng nổ của các website phishing. Thư rác hình (loại thư rác qua mặt các bộ lọc bằng cách nhúng hình ảnh vào trong phần nội dung email) cũng là một sản phẩm của Rock Phish.

Thậm chí, họ còn dự đoán rằng đến một ngày nào đó, riêng Rock Phish thôi, sẽ chiếm tới hơn một nửa số website phishing đang hoạt động của cả thế giới.

Đau đầu tìm giải pháp

Công nghệ scan chủ động đang là một hướng mà nhiều người nghĩ đến. Thay vì dựa dẫm vào danh sách đen, liệt kê những website phishing đã biết, công nghệ này phân tích hành vi cụ thể của một website bất kỳ, tìm kiếm những kỹ thuật, thủ pháp mà giới phisher thường sử dụng. Theo Microsoft, IE7 đã sử dụng công nghệ này.

Ngoài ra, giới bảo mật cũng ghi nhận sự nổi lên của một chuẩn xác thực site mới - có tên gọi EV SSL (hay Lớp bảo mật xác thực mở rộng). Để có được "con dấu xác nhận" này, một website sẽ phải chịu sự kiểm tra của một công ty trung gian như VeriSign hoặc Entrust để đảm bảo ít nhất, trông nó cũng có vẻ hợp pháp.

Sau khi "qua" được bài kiểm tra, tại những site này, thanh địa chỉ trình duyệt sẽ hiển thị màu xanh. Microsoft đã hỗ trợ EV SSL trong trình duyệt IE7, và nhiều site thương mại điện tử lớn như Pay-Pal cũng vừa bắt đầu ứng dụng chuẩn này.

Tuy nhiên, xin đừng mừng vội. Sự trỗi dậy khủng khiếp của các website phishing cho thấy: giới phisher có đủ mọi mánh khóe để qua mặt các công cụ lọc tự động. Gần đây nhất, chúng đã phát

triển được một số công nghệ mới, đe dọa cả những chuẩn bảo mật như EV SSL.

Cách bảo vệ tốt nhất

Hiện nay, người ta chưa tìm ra được liều thuốc thần dược nào để bảo vệ mình vô hại trước vấn nạn phishing. Mặc dù vậy, vẫn có một cách đơn giản để bạn tự bảo vệ lấy mình: không bao giờ click vào một bức email hay từ một website trung gian để đăng nhập vào tài khoản tài chính của mình.

Thay vào đó, hãy luôn sử dụng bookmark riêng hoặc chịu khó gõ đầy đủ địa chỉ website lên thanh địa chỉ trình duyệt, kể cả khi bạn dám chắc 100% rằng bức email là hợp pháp.

Các công cụ tự động như Password Safe cũng có thể trợ giúp phần nào. Tuy nhiên, để chống lại giới phisher tinh quái, phương án bảo vệ tốt nhất mà bạn có vẫn là... chính bạn.

Trọng Cầm