TẤN CÔNG PHISHING TĂNG MẠNH

MessageLabs (www.messagelabs.com) vừa công bố báo cáo về các phần mềm nguy hiểm tháng 8-2006, theo đó, phishing sẽ tiếp tục tăng với mánh khóe tinh vi hơn, chủ yếu nhằm mục đích đánh cắp tài khoản, thông tin cá nhân và cả các sản phẩm tr&iac

MessageLabs (www.messagelabs.com) vừa công bố báo cáo về các phần mềm nguy hiểm tháng 8-2006, theo đó, phishing sẽ tiếp tục tăng với mánh khóe tinh vi hơn, chủ yếu nhằm mục đích đánh cắp tài khoản, thông tin cá nhân và cả các sản phẩm trí tuệ. Báo cáo của MessageLabs nhắc nhở người sử dụng Internet phải cảnh giác với e-mail. Mark Sunner, giám đốc kỹ thuật của MessagLabs nói: "Làn sóng phising gần đây nhất sử dụng kỹ thuật "social engineering", tức là thu thập thông tin cá nhân từ site như MySpace. Bạn sẽ nhận được e-mail ngân hàng gửi riêng tới mình, với địa chỉ và mã vùng chính xác." MessageLabs đã phát hiện việc hacker tăng cường sử dụng phương pháp tấn công này từ tháng 12-2005. Trong khi đó, spam và virus nói chung không đáng sợ. Báo cáo trên cho biết các hình thức tấn công này đang giảm nhẹ. Theo ông Sunner, hiện virus thường đi kèm với spam. Tội phạm ảo sử dụng virus kèm Trojan để tạo ra các zombie (máy tính bị điều khiển), lập nên botnet (mạng các zombie) rồi mới tổ chức tấn công spam. Khi những đợt tấn công bằng virus lên đến đỉnh điểm vào mùa hè năm 2004, những botnet có trên 100.000 zombie không phải là hiếm, nhưng đến nay, botnet chỉ có khoảng 20.000 zombie hoặc ít hơn bởi bọn tội phạm muốn tránh lộ mặt. Tuy nhiên, các đợt tấn công qui mô nhỏ như hiện nay lại gây thiệt hại lớn hơn. MassageLabs cho biết cứ 321 e-mail họ chặn được thì có 1 spam. Mục tiêu chủ yếu hiện là các công ty thương mại. Những kẻ tấn công thường cài một Trojan vào các file tài liệu office và ngụy trang e-mail để người ta lầm tưởng nó được gửi từ một nguồn đáng tin cậy. Vậy phải đối phó với nguy cơ phishing ra sao? Theo ông Sunner, vấn đề là trong khi bọn tội phạm đã sử dụng những kĩ thuật tiên tiến nhất thì các công ty bảo mật lại vẫn phải dựa vào phương pháp vá lỗi đã có từ 20 năm nay. Việc "lọc" phải được thực hiện ngay trên internet, trước khi e-mail nguy hiểm tới được hòm thư. Ông Sunner cho biết: "Con người chính là điểm yếu nhất trong sợi xích bảo mật, nhưng thật không công bằng khi đổ hết trách nhiệm cho khách hàng. Việc lọc cần phải được thực hiện ngay ở "trên mây" (internet). Ví dụ, các nhà cung cấp dịch vụ phải lọc trước khi e-mail đến được người nhận." Ông cũng đặt ra câu hỏi: "Bạn không phải lọc nguồn cung cấp nước nếu có cặn bẩn, vậy tại sao bạn lại phải làm thế với việc duyệt internet?" HOÀNG MINH