TỘI PHẠM MẠNG: "LÀM ĂN NHỎ" AN TOÀN HƠN

Tội phạm mạng ngày nay tiến những bước nhỏ hơn và chú trọng đến các cuộc tấn công có mục tiêu nhiều hơn nhằm tránh bị phát hiện và thu được nhiều lợi nhuận hơn. Bản báo cáo "Các mối đe doạn bảo mật Internet" của Symantec công bố ngày h&oc

Tội phạm mạng ngày nay tiến những bước nhỏ hơn và chú trọng đến các cuộc tấn công có mục tiêu nhiều hơn nhằm tránh bị phát hiện và thu được nhiều lợi nhuận hơn. Bản báo cáo "Các mối đe doạn bảo mật Internet" của Symantec công bố ngày hôm qua cho biết, trong nửa cuối năm 2005, bọn tội phạm mạng đã chuyển mục tiêu từ các cuộc tấn công lớn rộng khắp nhằm đột phá tường lửa và bộ định tuyến mạng sang mục tiêu là các máy tính để bàn và ứng dụng web thông qua phương thức ăn cắp thông tin tài chính cá nhân. Con số thống kê trong bản báo cáo của Symantec cũng cho thấy các phần mối đe doạ bảo mật nưhư virus, sâu máy tính và trojan chuyên ăn cắp thông tin bí mật của người sử dụng đã chiếm tới 80% trong số Top 50 phần mềm độc hại nhất. Con số này đã tăng thêm 6% so với con số của 6 tháng đầu năm 2005. Lừa đảo trực tuyến như tấn công phishing lừa người sử dụng tiết lộ các thông tin bí mật như mật khẩu, thông tin thẻ tín dụng và các thông tin tài chính khác cũng tăng mạnh. Số liệu thống kê cho thấy, trong khoảng thời gian từ ngày 01/07 đến hết ngày 31/12/2005, cứ trong 119 bức thông điệp điện tử được xử lý thì có 1 email phishing. Con số này đã đã đẩy mức email phishing bình quân mỗi ngày lên tới 7,92 triệu - tăng 2,22 triệu so với con số của sáu tháng đầu năm. Vincent Weafer - giám đốc cao cấp của Symantec Security Response - cho biết tin tặc đang dần chuyển từ việc phát tán các loại virus hay sâu máy tính có khả năng lây nhiễm hàng trăm hàng nghìn máy tính khác nhau sang chú trọng đến các cuộc tấn công quy mô nhỏ hơn. Vincent cho rằng tội phạm mạng hiện không muốn "gây chiến" với các đội phản ứng bảo mật của các hãng bảo mật trên toàn thế giới bằng các cuộc tấn công "nổi tiếng" mà giờ đây chúng muốn tấn công bí mật lên hệ thống của người sử dụng hơn. Minh chứng cho điều này, Vincent khẳng định, là các loại virus mà mỗi khi xuất hiện là nổi đình nổi đám trên các trang báo chí như thời của sâu Blaster đã giảm đi một cách đáng kể. "Thay vì gửi đi một con sâu máy tính có khả năng lây nhiễm lên hàng nghìn máy tính để bàn, thì bọn tội phạm lại đang tổ chức những cuộc tấn công nhỏ lẻ hơn nhưng nguy hiểm hơn. Đơn giản vì chúng muốn đột nhập lên hệ thống của người sử dụng một cách bí mật." Bản báo cáo "Các mối đe doạn bảo mật Internet" cũng cho biết các mối đe doạn từ các hệ thống mạng "bot" - hệ thống mạng được sử dụng để tổ chức các cuộc tấn công - đang gia tăng mạnh mẽ. Tội phạm mạng thường tạo nên công cụ này bằng việc chiếm quyền điều khiển bất hợp pháp một số lượng lớn các máy tính khác nhau. Mỗi ngày Symantec thống kê được tổng cộng 1.402 cuộc tấn công từ chối dịch vụ bằng cách sử dụng các botnet - tăng hơn 51% so với bản báo cáo lần trước. Trung Quốc hiện đang dần trở thành một "nguồn gốc" chính của các cuộc tấn công bằng các mạng "bot" khi mà tốc độ phát triển mạng băng thông rộng tại nước này đang trong quá trình tăng trưởng mạnh mẽ.