NHỨC NHỐI AN NINH MẠNG TẠI VIỆT NAM

1,4 triệu máy tính bị nhiễm virus "nội" trong một tuần đầu tháng 9/2006, hàng trăm trang web bị hacker trong nước và nước ngoài tấn công là vài con số về tình trạng an ninh mạng ở Việt Nam. Trung tâm Ứng cứu Khẩn cấp Máy tính Quốc gia (VNCERT) cho b

1,4 triệu máy tính bị nhiễm virus "nội" trong một tuần đầu tháng 9/2006, hàng trăm trang web bị hacker trong nước và nước ngoài tấn công là vài con số về tình trạng an ninh mạng ở Việt Nam. Trung tâm Ứng cứu Khẩn cấp Máy tính Quốc gia (VNCERT) cho biết sẽ tập trung vào việc điều phối để đối phó nhanh chóng với những vấn đề an ninh trên môi trường mạng. Sốt dịch virus "nội" Theo VNCERT, ước tính có khoảng 1,4 triệu máy tính ở Việt Nam đã bị nhiễm các virus "nội" phát tán qua dịch vụ chat Yahoo! Messenger trong khoảng một tuần đầu tháng 9/2006. Đây là con số tương đối bất ngờ bởi theo thống kê mới đây của Trung tâm An ninh mạng Bách Khoa (BKIS), có khoảng 550.000 máy tính ở Việt Nam đã bị nhiễm các virus "nội" xuất hiện trong tháng 9.

Nguồn: typepad

Giải thích về con số trên, VNCERT cho biết ngay sau khi xuất hiện các virus phát tán qua Yahoo! Messenger vào đầu tháng 9, trung tâm này đã gửi một công văn đề nghị 6 ISP lớn phối hợp ngăn chặn sự lây lan của các virus này. Theo VNCERT, các virus phát tán của Yahoo1 Messenger chủ yếu lây lan từ một vài tên miền đặt ở nước ngoài. Do đó, nếu chặn kết nối đến các tên miền này có thể chấm dứt sự phát tán của các virus. Ngay sau công văn của VNCERT, NetNam cho biết, chỉ trong một ngày, công ty đã ghi nhận được khoảng 5000 lượt truy xuất vào 6 nguồn phát tán virus từ hệ thống của NetNam. NetNam là ISP nhỏ, chiếm 2,58 thị phần thuê bao Internet. Nếu tính quy đổi các ISP còn lại theo cách đơn giản, số lượng máy tính ở Việt Nam bị nhiễm các virus này ước khoảng 200.000 máy tính trong một ngày, và trong một tuần là 1,4 triệu máy tính bị nhiễm. Một đại diện của VNCERT cho rằng, nếu giả định mỗi máy tính mất khoảng 2 USD chi phí khắc phục hậu quả, chúng ta đã mất khoảng 2,8 triệu USD (hơn 40 tỷ đồng) vì mấy con virus "nội" này. Đó là chưa kể nếu các virus này phá hoại dữ liệu thì hậu quả sẽ không thể nào đo đếm được, đại diện VNCERT cho biết. Theo thống kê của BKIS, chỉ trong tháng 9/2006, có tới 10 virus "nội" lây lan qua Yahoo! Messenger liên tiếp tung được lên mạng. Tháng 9 cũng là tháng kỷ lục về số lượng virus, trung bình mỗi ngày xuất hiện 3 virus mới. Tội phạm bắt đầu chuyên nghiệp Mấy ngày vừa qua, hàng loạt tên miền của Chợ điện tử, sàn giao dịch thương mại điện tử của Công ty Giải pháp Phần mềm Hoà Bình liên tiếp bị hacker tấn công chiếm đoạt tên miền. Cuộc tấn công vào Chợ điện tử kéo dài liên tiếp trong vòng 10 ngày cuối tháng 9/2006 khiến công ty này phải từ bỏ tên miền quốc tế, chuyển mọi hoạt động về tên miền .vn. Ông Nguyễn Tử Quảng cho biết BKIS đang phối hợp với đơn vị phòng chống tội phạm công nghệ cao điều tra. Tuy nhiên, theo ông Quảng cho

biết, những ghi nhận ban đầu cho thấy đây là vụ tấn công được chuẩn bị rất kỹ lưỡng, có thể có sự tham gia của nhiều hacker.

Website Chợ điện tử liên tiếp bị tấn công

Trước đó, trang web thương mại điện tử của công ty Việt Cơ và trang web của công ty Nhân Hòa cũng đã bị tấn công từ chối dịch vụ, làm ngưng trệ hoạt động trong thời gian dài. Tháng 5/2006, trang web của VMS Mobifone bị tấn công thất thoát thông tin, sau đó một tháng trang web của VDC cũng bị hack. Vào tháng 1/2006, đơn vị điều tra tội phạm công nghệ cao, Bộ Công an đã bắt giữ đường dây ăn cắp thẻ tín dụng quốc tế. Zone-H (địa chỉ thống kê những trang web bị hacker tấn công) đã liệt kê 30 trang web của các cơ quan chính phủ (.gov.vn), 10 trang web doanh nghiệp và gần 20 trang web .vn khác đã bị hacker tấn công từ tháng 6 đến cuối tháng 9/2006. Tháng 8/2006, BKIS đã thực hiện khảo sát đánh giá độ an toàn với 200 trang web ở Việt Nam. Kết quả có tới 50 trang web mắc những lỗi bảo mật nghiêm trọng, phần nhiều trong số này là các trang web .gov.vn. Có thể nói, tình trạng an ninh mạng từ đầu năm đến nay luôn nóng bỏng. Tuy nhiên, theo ông Đỗ Ngọc Duy Trác, phụ trách nghiệp vụ của VNCERT, đáng ngại hơn là tội phạm máy tính đã bắt đầu hình thành các hoạt động giống với tội phạm quốc tế, mang dáng dấp tội phạm chuyên nghiệp. “Mấy năm trước tội phạm máy tính phổ biến là ăn cắp mật khẩu tín dụng mua sách qua mạng, gần đây đã tiến tới làm thẻ tín dụng giả để rửa tiền, hình thành các mạng máy tính ma để gửi thư rác, thư quảng cáo, tấn công từ chối dịch vụ, thậm chí đã có dấu hiệu của hoạt động bảo kê tống tiền các trang web thương mại”, ông Trác nói. Vai trò điều phối quốc gia Với đà phát triển ứng dụng CNTT-TT hiện nay, ông Vũ Quốc Khánh, Giám đốc VNCERT cho rằng thiệt hại do mất an toàn mạng sẽ tăng nhanh và ảnh hưởng nghiêm trọng đến phát triển kinh tế nếu việc đảm bảo an ninh mạng không được triển khai đủ mức. Ông Khánh cho biết, VNCERT đang hoàn thành chiến lược về an toàn thông tin trên môi trường mạng, trong đó sẽ đưa ra những biện pháp đối phó nhanh chóng với những vấn đề ảnh hưởng đến an toàn thông tin trên mạng. Dự kiến, những công việc VNCERT sẽ triển khai từ nay đến năm 2010 là xây dựng các hệ thống cảnh báo sớm những vấn đề an ninh mạng, hệ thống hỗ trợ điều tra sự cố và tội phạm mạng, hệ thống khắc phục điểm yếu, hệ thống thu thập thông tin, giám sát và thống kê dữ liệu. Bên cạnh đó, VNCERT cũng sẽ chủ động xây dựng cơ chế điều phối, tham gia xây dựng hành lang pháp lý cho vấn đề an ninh mạng, xây dựng các tiêu chuẩn an toàn thông tin và triển khai các chương trình nâng cao nhận thức cộng đồng về an ninh thông tin trên môi trường mạng. Tuy nhiên, “trước mắt trung tâm này sẽ tập trung mạnh vào hoạt động điều phối để nhanh chóng giải quyết những vấn đề an ninh mạng,” ông Khánh cho biết. Theo đại diện VNCERT, những hoạt động điều phối bước đầu của trung tâm đã mang lại hiệu quả rõ rệt. Ví dụ, mới đây nhất trong vụ

trang web của Chợ điện tử bị tấn công, VNCERT đã nhanh chóng yêu cầu các ISP tiến hành cô lập quá trình phân giải tên miền của Chodientu.com trong khi chờ đợi Register.com (nơi Chợ điện tử đăng ký tên miền) khắc phục sự cố và yêu cầu các ISP trong nước ngăn chặn truy xuất vào nguồn đang phát tán virus. Do đó, trang web của Chodientu nhanh chóng trở lại hoạt động bình thường mặc dù Register.com vẫn chưa khắc phục xong sự cố. Trước đó, vào đầu tháng 9/2006, nhằm hạn chế sự phát tán của các virus "nội" lây lan qua Yahoo! Messenger, VNCERT đã gửi một văn bản yêu cầu sự phối hợp của các ISP trong nước. Ông Trác cho rằng nếu các ISP nghiêm túc thực hiện yêu cầu ngăn chặn kết nối đến các nguồn phát tán các virus này, thì chỉ trong vài phút có thể chặn đứng sự lây lan. "Nhưng có lẽ đây là vấn đề chưa có tiền lệ, nên một số ISP không tích cực phối hợp", ông Trác cho biết. Tuy nhiên, đại diện VNCERT khẳng định, sắp tới trung tâm này sẽ đưa ra những quy chế ràng buộc, yêu cầu các ISP phối hợp trong việc đối phó với những vấn đề an toàn thông tin trên môi trường mạng. Đỗ Duy