1.493 VIRUS MỚI XUẤT HIỆN TRONG THÁNG 3

Trong

Trong tháng 3, có 3.829.000 máy tính bị nhiễm virus và 1.493 virus mới xuất hiện. Đây là con số đáng báo động về an ninh mạng trong thời điểm này.

100% virus xuất hiện trong tháng 3 có xuất xứ nước ngoài

Theo thống kê từ hệ thống giám sát virus của Bkav, tất cả 1.493 virus mới xuất hiện trong tháng 3 đều có xuất xứ từ nước ngoài. Trong đó nhiều nhất là các virus xuất xứ từ Trung Quốc, Mỹ, Ukraine và Nga.

Năm 2007, trong số 6.752 virus mới xuất hiện tại Việt Nam chỉ có 14 virus xuất xứ từ Việt Nam (chiếm 0,2 %).

Với môi trường Internet, sự phát tán của virus hiện nay không phụ thuộc vào vị trí địa lý của các quốc gia. Người sử dụng ở Việt Nam hay ở một nước nào khác cũng đều phải đối mặt với những nguy cơ về virus như nhau, bất kể nguồn xuất xứ của virus. Chính vì vậy, để phòng chống virus hiệu quả, người sử dụng cần lựa chọn phần mềm diệt virus có khả năng cập nhật kịp thời nhất những mẫu virus mới xuất hiện.

Virus Dasher tiếp tục lây tràn lan

Virus chèn banner tiếng Trung Quốc Dashfer vẫn lây tràn lan trong hệ thống mạng của nhiều cơ quan, doanh nghiệp tại Việt nam. Nếu một máy tính trong mạng bị nhiễm Dashfer, các máy tính khác trong mạng đều gặp phải hiện tượng bị chèn banner. Chính vì vậy, không phải máy tính nào có hiện tượng trên cũng là máy bị nhiễm virus.

Điều này đã gây rất nhiều khó khăn cho các quản trị mạng trong việc tìm và khống chế các máy tính bị nhiễm virus trong mạng. Không những thế, máy tính bị nhiễm còn có thể kiểm soát được toàn bộ quá trình trao đổi dữ liệu của các máy tính khác. Đây cũng là một trong những nguy cơ mất an ninh thông tin nghiêm trọng cho các doanh nghiệp.

Trung tâm An ninh mạng BKIS cho biết, để xử lý triệt để loại virus chèn banner này, các quản trị mạng phải rà soát và xử lý virus trên tất cả các máy tính trong mạng. Cách tốt nhất là trang bị cho cơ quan một giải pháp phòng chống virus tổng thể.

Lỗ hổng Zero-day đe dọa an ninh mạng của các doanh nghiệp

Trong tháng 3, một số phần mềm phổ biến xuất hiện lỗ hổng Zero-day. Sở dĩ, những lỗ hổng này được gọi là Zero-day vì tại thời điểm lỗ hổng được công bố, nhà sản xuất phần mềm chưa kịp đưa ra bản vá lỗi, và người sử dụng không được bảo vệ trước những lỗ hổng này.

Điển hình là lỗ hổng nghiêm trọng trong phần mềm mail server Mdeamon phiên bản từ 9.6.4 trở về trước. Đây cũng là phần mềm được sử dụng phổ biến tại Việt Nam.

Khai thác lỗ hổng của giao thức IMAP trong Mdaemon phiên bản 9.6.4 trở về trước, hacker có thể chiếm toàn bộ quyền điều khiển máy chủ. Hơn một tuần sau khi lỗ hổng được công bố, nhà sản xuất mới đưa ra bản vá. Hiện tại còn nhiều cơ quan, doanh nghiệp tại Việt Nam chưa cập nhật bản vá lỗ hổng này, do đó hệ thống mạng vẫn đứng trước nguy cơ bị hacker kiểm soát.

Đây là mối hiểm họa khôn lường đối với hệ thống thông tin của các doanh nghiệp. Để hạn chế sự phát tác, các doanh nghiệp cần thường xuyên theo dõi tin tức an ninh mạng để có phản ứng kịp thời.