TROJAN TẤN CÔNG LỖ HỔNG CHƯA ĐƯỢC VÁ CỦA WINDOWS

“Cha đẻ” của các loại virus toàn cầu đang tích cực khai thác lỗ hổng bảo mật trong Microsoft Jet Database Engine của hệ điều Windows - một lỗ hổng đã bị bỏ quên không được vá trong suốt 5 tháng qua kể từ khi Microsoft lần đầu tiên nhận được thông báo. C&aacu

“Cha đẻ” của các loại virus toàn cầu đang tích cực khai thác lỗ hổng bảo mật trong Microsoft Jet Database Engine của hệ điều Windows - một lỗ hổng đã bị bỏ quên không được vá trong suốt 5 tháng qua kể từ khi Microsoft lần đầu tiên nhận được thông báo. Các chuyên gia bảo mật đã xếp lỗ hổng bảo mật trong động cơ quản trị dữ liệu Microsoft Jet – ứng dụng được sử dụng khá phổ biến trong các phần mềm như as Microsoft Office 2000, Office 2003, Access 2000 và Access 2003 – vào mức “cực kì nguy hiểm” nhưng Microsoft dường như đã quên mất vấn đề này. Để khai thác lỗ hổng này các loại virus thường sử dụng tệp tin mạo danh Microsoft Access để đột nhập vào máy tính của các nạn nhân. Tháng 3 vừa qua, Microsoft đã nhận được những thông báo về lỗ hổng bảo mật này cùng với cảnh báo là tin tặc hoàn toàn có thể lợi dụng lỗ hổng này để đột nhập và chiếm quyền kiểm soát máy tính của người sử dụng. Tuy nhiên, Microsoft lại chưa hề cho công bố lỗi trong Jet database engine mặc dù biết các hệ thống sử dụng Microsoft Access 2003 và Microsoft Windows XP - kể cả Windows XP SP2 - đều bị ảnh hưởng bởi lỗ hổng này. Tuy nhiên, theo cảnh báo của hãng bảo mật Symantec thì đến nay mới có duy nhất con trojan Backdoor.Hesive là nhắm mục tiêu khai thác lỗ hổng này. Hãng bảo mật đánh giá khả năng phát tán của Hesive là thấp nhưng vẫn cảnh báo về khả năng gây thiệt hại tiềm tàng của loại trojan này. Người sử dụng các hệ điều hành Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP và Windows Server 2003 đều nằm trong tầm ảnh hưởng của Hesive. Một khi đã đột nhật vào máy tính của nạn nhân, con trojan này sẽ mở một cổng sau cho phép tin tặc có thể từ xa chiếm quyền điều khiển máy tính của người sử dụng. Kiểu tấn công như thế này thường là để đặt nền tảng gieo mầm mống nuôi các các PC zombies phục vụ cho mục đích spam hay phát tán phần mềm nguy hiểm. Microsoft hiện vẫn chưa có bất kỳ phản ứng chính thức nào về việc này. HVD - (eWeek)