SÂU OPENOFFICE TẤN CÔNG LIÊN HỆ ĐIỀU HÀNH

Hãng b

Hãng bảo mật Symantec cảnh báo một mã độc tấn công OpenOffice.org có khả năng lây nhiễm lên nhiều hệ điều hành khác nhau lại vừa được tin tặc tung lên mạng Internet.

Thông tin từ Symantec Security Response cho biết thực chất mã độc nói trên là một con sâu máy tính đính kèm trong các tệp tin OpenOffice độc hại được phát tán bằng con đường email. Con sâu này có khả năng lây nhiễm lên hệ điều hành Windows, Linux và Mac OS X.

Con sâu máy tính này đã được phát hiện hồi cuối tháng trước. Tuy nhiên tại thời điểm đó các chuyên gia bảo mật cho rằng chúng chưa được phát tán rộng trên mạng Internet.

Nếu người dùng mở tệp tin OpenOffice độc hại con sâu badbunny.odg ngay lập tức sẽ được khởi động cùng với một macro có chức năng xác định hệ điều hành mà người dùng đang sử dụng.

Nếu đó là hệ điều hành Windows, con sâu sẽ cấy một tệp tin có tên "drop.bad" vào hệ thống. Chức năng chính của tệp tin này là di chuyển tệp tin hệ thống the system.ini vào trong thư mục mIRC. Đồng thời nó cũng cho thực thi một JavaScript badbunny.js có chức năng nhân bản các tệp tin khác trong thư mục nó tồn tại.

Còn trên hệ điều hành Mac OS X con sâu cấy vào đây hai con virus Ruby Script có tên "badbunny.rb" và "badbunnya.rb". Hệ thống Linux thì bị nhiễm hai con virus XChat Script "badbunny.py" và Perl Script "badbunny.pl".

Symantec xếp con sâu OpenOffice mới vào mức nguy hiểm trung bình. Hãng bảo mật khuyến cáo người dùng không nên mở các tệp tin OpenOffice được gửi đến từ một nguồn không rõ ràng.

Hoàng Dũng