TIN TẶC PHÁT TÁN MÃ ĐỘC TẤN CÔNG WORD

Thường

Thường không lâu sau khi Microsoft phát hành bản cập nhật hàng tháng khắc phục lỗi bảo mật trong các sản phẩm phần mềm thì tin tặc cũng ngay lập tức phát hành mã độc tấn công những lỗi đó. Mục tiêu mà chúng nhắm đến là những PC chưa được cài đặt các bản vá lỗi.

Với tháng 10 lần này lỗi bảo mật được tin tặc nhắm đến là lỗi thuộc về ứng dụng xử lý văn bản Microsoft Word. Đây là một lỗi tràn bộ nhớ đệm. Các chuyên gia bảo mật cho biết lỗi tràn bộ nhớ đệm rất dễ bị lợi dụng để chạy mã độc trên hệ thống mắc lỗi nếu khai thác thành công.

Trước khi Microsoft phát hành bản vá, lỗi này đã từng bị lợi dụng để tấn công người dùng trước đây. Song sau khi bản vá phát hành lỗi này càng bị lợi dụng nhiều hơn.

Hãng bảo mật Symantec cho biết lỗi bảo mật Word giờ bị lợi dụng để tấn công người dùng trong những vụ tấn công có phạm vi rất rộng. Ít nhất tính đến thời điểm này những tệp tin Word độc hại phát tán trên mạng Internet mang trong mình hàng loạt mã shell cho phép thực thi ứng dụng cộng thêm 3 mã độc khác.

Những mã độc này gồm 2 con trojan Trojan-Dropper và Backdoor-Trojan. Trong đó Backdoor-Trojan chịu trách nhiệm mở một cổng bí mật trên PC mắc lỗi để Trojan-Dropper có thể tải về thêm nhiều mã độc khác hơn. Mã độc thứ ba chính là Hacktool-Rootkit có chức năng chính là che giấu mã độc trước "con mắt giám sát" của các phần mềm bảo mật.

Ngoài ra, Symantec còn nhấn mạnh phương thức tấn công lần này thực sự khác biệt. Thay vì tạo ra những tệp tin chuẩn định dạng Windows OLE, lần này tin tặc lại tạo ra chuẩn định Word ứng dụng riêng cho hệ điều hành Apple Mac OS.

Nhưng dù thế nào đi chăng nữa thì mục tiêu chính của tin tặc chính là tấn công người dùng Windows thông qua lỗ hổng bảo mật mới được công bố chi tiết.

Song vẫn có một tin mừng đối với người dùng là phiên bản Microsoft Office 2007 và Office 2003 Service Pack 3 không tương thích mới chuẩn định dạng Word Mac OS, chính vì thế mà những phiên bản này miễn dịch với các vụ tấn công lần này.

Người dùng được khuyến cáo là không nên mở các tệp tin Word được gửi đến từ những nguồn

không rõ ràng và nên nhanh chóng tải về cài đặt các bản vá lỗi cần thiết.

Hoàng Dũng