TROJAN GIẢ MẠO CẢNH BÁO BẢO MẬT CỦA MICROSOFT

Một ch

Một chiến dịch tấn công thư rác mạo danh bản tin cảnh báo bảo mật của Microsoft vừa được tin tặc khởi động với mục tiêu lừa người dùng tải về và cài đặt một con trojan nguy hiểm.

Những email thường mang tựa đề "Cumulative Security Update for Internet Explorer" giả mạo cung cấp bản vá lỗi nguy hiểm cho trình duyệt Internet Explorer. Có đường liên kết cụ thể cho phép người dùng tải về bản vá.

Nếu người dùng nhắp chuột vào đường liên kết đó họ sẽ được kết nối đến một máy chủ ở xa và tải về một con trojan có tên Trojan-Downloader.Win32.Agent.avk. Chức năng chính của con trojan này là cầu nối giúp nhiều loại phần mềm độc hại khác xâm nhập vào hệ thống bị nhiễm.

Chuyên gia nghiên cứu Lenny Zeltser của SANS Internet Storm Center - hãng phát hiện ra đợt tấn công này - nhận định mục tiêu của tin tặc trong chiến dịch lừa đảo lần này có thể là những tên miền và máy chủ chúng đang cần để tiếp tục mở rộng việc tấn công.

Những vụ tấn công kiểu như thế này hiện vẫn lừa được không ít người dùng. Thường người dùng không để ý đến những khác biệt giữa một bản tin cảnh báo chính thống và giả mạo cho dù sản phẩm giả mạo chứa những lỗi rất dễ bị phát hiện.

Người dùng cần chú ý một điều Microsoft không bao giờ gửi bản tin cảnh báo thông qua email trước khi hãng phát hành bản cập nhật định kỳ hàng tháng. Thêm vào đó đường liên kết đến bản vá lỗi sẽ dẫn người dùng đến chính trang cung cấp thông tin đầy đủ về bản vá chứ không phải là một tệp tin.

Hoàng Dũng