HIỂM HOẠ TỪ WEB QUA MẶT EMAIL ĐỘC HẠI

Hãng b

Hãng bảo mật Trend Micro dự báo sang năm tới số lượng các vụ tấn công bắt nguồn từ web sẽ nhiều hơn từ email.

Email hiện đã được xem là phương thức tấn công truyền thống. Trojan và các dạng phần mềm độc hại thường được giấu trong các email chui vào hộp thư của người dùng rồi từ đó đột nhập vào PC người dùng.

Nhưng tình thế hiện nay đã bắt đầu có sự biến chuyển. Web đang dần trở thành công cụ "ưa thích" để tấn công PC của giới tin tặc.

Phát biểu trước các đại biểu tham gia Gartner Symposium & ITxpo, ông Raimund Genes - Giám đốc nghiên cứu của Trend Micro - khẳng định sang năm 2008 hầu hết các hiểm hoạ đe doạ người dùng Internet sẽ được đưa lên web.

Nguyên nhân của sự chuyển đổi xu hướng rất đơn giản. Hiện các công cụ bảo mật email đã trở nên quen thuộc với người dùng. Trong khi đó hiện nay gần như chưa có công cụ bảo mật kiểm soát lưu lượng dữ liệu mạng. Các hãng bảo mật cũng phải thừa nhận vấn đề bảo đảm an toàn cho những gì xâm nhập vào PC và hệ thống mạng thông qua cổng 80 là một nhiệm vụ không hề đơn giản.

Minh chứng cho mức độ nguy hiểm của hiểm hoạ trên web ông Genes đưa ra ví dụ về trường hợp website Dolphin Stadium. Trang web này đã bị giới tin tặc bắt cóc và lợi dụng để cài đặt phần mềm độc hại lên PC người dùng.

Trò chơi mèo đuổi chuột

Tình thế giữa hãng bảo mật và tin tặc giống hệt trò chơi mèo đuổi chuột. Tin tặc tìm kiếm những lỗ hổng bảo mật mới những công cụ những phần mềm độc hại mới để tấn công người dùng còn các hãng bảo mật thường phải đi theo sau dọn dẹp.

Thậm chí ngày nay giới tin tặc còn hình thành nên một thị trường chợ đen chuyên buôn bán những lỗi bảo mật.

"Lợi nhuận thu được từ các loại mã độc chính là nguyên nhân thúc đẩy sự phát triển của các hiểm hoạ web," ông Genes nhận định. "Con virus máy cuối cùng xuất hiện năm 1999. Rồi kể từ đó đến nay chỉ có sâu máy tính và hiểm hoạ web".

Ví dụ giới tin tặc sẵn sàng trả tới 75.000 USD cho một lỗi bảo mật trong hệ điều hành Windows XP và 50.000 cho lỗi trong Windows Vista. Thậm chí ngay cả những hãng bảo mật như iDefense hay TippingPoint cũng treo giải 12.000 cho một lỗi bảo mật.

Không phải ngành bảo mật thế giới không quan tâm tới những hiểm hoạ web bởi công việc bảo đảm giao thông mạng doanh nghiệp an toàn đã có những hãng chuyên trách như Websense, Surf Control và ScanSafe. Những hãng này đều có các sản phẩm cho phép khoá chặn những luồng dữ liệu web độc hại.

"Nhưng một sự thật là hiện các hãng bảo mật vẫn chưa thể đuổi kịp giới tin tặc. Bảo mật thường phải đuổi bắt giới tin tặc chứ chưa thể chặn đầu chúng," ông Genes cho biết.

Hoàng Dũng