SYMANTEC TÍCH HỢP CÔNG CỤ CHỐNG TẤN CÔNG "ZERO-DAY" VÀO ỨNG DỤNG

Bắt đầ

Bắt đầu từ tháng tới, người dùng các sản phẩm Norton của Symantec sẽ có thêm một công cụ mới để loạt bỏ các nguy cơ phát sinh từ những lỗ hổng phần mềm chưa được sửa chữa.

Có tên là "Symantec online Network for Advanced Response" (SONAR), phần mềm bảo mật mới sẽ theo dõi các hành vi chương trình chạy trên hệ thống để xác định xem chúng có thuộc loại nguy hiểm không. SONAR là một dạng cao cấp hơn của kỹ thuật diệt virus dựa trên chữ ký truyền thống của Symantec (so sánh chữ ký của chương trình với cơ sở dữ liệu các loại phần mềm độc hại được ghi nhận trước đó).

SONAR sẽ là một dạng add-on miễn phí dành cho ứng dụng Norton AntiVirus 2007 và Norton Internet Security 2007 của Symantec. "Chúng tôi rất vui mừng giới thiệu SONAR. Nó sẽ là một phương pháp bảo vệ chống lại các cuộc tấn công zero-day không dựa trên chữ ký mã độc", phát biểu của ông Ed Kim, giám đốc quản lý sản phẩm đơn vị kinh doanh khách hàng của Symantec.

Các cuộc tấn công zero-day thường dựa trên những lỗ hổng chưa được công bố, hoặc chưa được các hãng phần mềm sửa chữa, và thường rất hiệu quả đối với những dạng bảo vệ bằng kho cơ sở dữ liệu diệt virus dựa trên chữ ký.

SONAR sử dụng thuật toán để đánh giá hàng trăm thuộc tính liên quan tới một phần mềm chạy trên hệ thống để phát hiện một phần mềm nguy hiểm, đã hoặc chưa được Symantec và các nhà nghiên cứu bảo mật khác xác định.

SONAR xác định một phần mềm có thuộc loại "độc hại" hay không dựa trên hành vi chứ không dựa trên kho dữ liệu đã được quy định trước đó về phần mềm. Chẳng hạn một chương trình có chức năng bổ sung shortcut ra desktop, hoặc tự chèn vào danh sách chương trình Windows Add/Remove sẽ được xác định là chương trình độc hại.