SYMANTEC CŨNG SỬ DỤNG TÍNH NĂNG ROOTKIT

Symantec đã sử dụng một tính năng trong bộ tiện ích cho hệ thống là Norton SystemWorks sử dụng một kỹ thuật giống với rootkit để ẩn một thư mục hệ thống trong Windows.

Công nghệ này hoạt động cũng gần giống với DRM rootkit đang bị phản đối gay gắt của Sony BMG theo cách thức mà nó đánh dấu tập tin và ẩn giấu chúng với hệ điều hành.

Tính năng Norton Protected Recycle Bin bổ sung thêm một thư mục được gọi là NProtect sẽ lưu trữ tạm thời những tập tin mà người dùng xóa đi. Ý tưởng này nhằm bổ sung thêm cho thùng rác (Recycle Bin) của Windows và người dùng có thể khôi phục lại các tập tin đã xóa.

Tuy nhiên, ẩn đi một thư mục từ Windows có thể mở một "cửa hậu" cho các lỗi bảo mật như sự sụp đổ của Sony DRM Rootkit. Những kẻ lợi dụng có thể viết các virus và sâu mới được ẩn giấu trong lốt thư mục nhằm tránh việc dò tìm từ các phần mềm bảo mật nhận biết chúng có mặt trên máy tính.

"NProtect sẽ vẫn tiếp tục chức năng hoạt động của mình như trước và người dùng cũng sẽ có thể kích hoạt hay tắt chức năng thông qua giao diện quản lý Norton Protected Recycle Bin", Symantec cho biết.

Người dùng Norton SystemWorks có thể tải về phiên bản vá lỗi thông qua chức năng LiveUpdate.

"Symantec không quan tâm đang các âm mưu của hacker để giấu giếm mã hiểm độc trong thư mục NProtect. Phần cập nhật này nhằm cung cấp khả năng loại trừ những nguy cơ có thể xảy ra".

Được khám phá bởi Mark Russinovich của Sysinternals, người đầu tiên phát hành chi tiết về phần mềm Sony XCP. Symantec cũng tỏ lời cám ơn đến nhóm F-Secure Blacklight về sự giúp sức giải quyết vấn đề này.

Người dùng có thể tham khảo thêm thông tin tại đây.