VISTA SẼ LÀ "TỬ THÙ" CỦA PHẦN MỀM DIỆT VIRUS?

Tính năng bảo vệ bản quyền số bên trong hệ điều hành Windows mới có thể cho phép hacker dễ dàng trói tay các ứng dụng diệt virus, không cho chúng thực thi phận sự xóa bỏ malware của mình. Trong bài thuyết trình tại Hội thảo Bản tin Virus thường niê

Tính năng bảo vệ bản quyền số bên trong hệ điều hành Windows mới có thể cho phép hacker dễ dàng trói tay các ứng dụng diệt virus, không cho chúng thực thi phận sự xóa bỏ malware của mình. Trong bài thuyết trình tại Hội thảo Bản tin Virus thường niên đang diễn ra tại Montreal, Canada, chuyên gia Aleksander Czarnowski của hãng bảo mật AVET cảnh báo rằng tính năng Bảo vệ bản quyền số (DRM) bên trong Vista có thể bị hacker lợi dụng để bảo vệ chính ... rootkit và các đoạn mã độc hại.

Nguồn: CNET

Khi tính năng này kích hoạt, nó sẽ tạo ra một "chương trình được bảo vệ " tựa như ấu trùng vậy. "Ấu trùng" có thể chạy song song, cùng lúc với những chương trình khác bên trong một hệ điều hành multitask như Windows. Trong khi các chương trình bình thường có thể bị chương trình "mẹ" điều khiển (chương trình mẹ là quy trình có quyền ưu tiên cao, hoặc do người dùng có quyền admin tạo ra), thì "ấu trùng" giống như một ốc đảo, cô lập với cả hệ thống. Sự tương tác giữa "ấu trùng" với các chương trình bình thường bị hạn chế tới mức tối đa. Lấy thí dụ, một chương trình thường sẽ không thể gửi thread đến cho "ấu trùng", cũng như không thể truy cập vào bộ nhớ ảo mà "ấu trùng" đang sử dụng. Những hạn chế này phục vụ đắc lực cho việc quản lý bản quyền số, vì nó kiểm soát chặt chẽ các hoạt động truy cập, phát tán nội dung truyền thông. Thế nhưng mặt trái của nó là tạo ra môi trường lý tưởng cho malware ẩn nấp, thách thức các phần mềm diệt virus bên ngoài. Ngay quyền ưu tiên của admin cũng không can thiệp được vào các quy trình ấu trùng. Các phần mềm diệt virus sẽ không thể phân tích được những thay đổi bên trong hệ thống để từ đó phát hiện ra dấu vết malware. Lấy thí dụ, nếu một phần mềm phá hoại có thể điều khiển được quy trình "ấu trùng", nó sẽ có thể sử dụng ấu trùng để chỉnh sửa địa chỉ bộ nhớ và "vô hình" hóa tất cả các thay đổi này trong mắt phần mềm bảo mật. Dù đang chạy song song trong cùng một môi trường máy tính nhưng các công cụ quét virus vẫn phải "bó tay". "Tôi nghĩ là họ chưa lường hết hậu quả của việc trao tính năng này vào tay kẻ xấu", Czarnowski cảnh báo. "Quy trình ấu trùng là một vũ khí, và cũng như mọi vũ khí khác, nó có thể được sử dụng vào cả mục đích tốt lẫn mục đích xấu". Phía Microsoft chưa đưa ra bất cứ bình luận nào, song có vẻ như hãng đã biết về nguy cơ này. Czarnowski khẳng định ông chưa ghi nhận được bất cứ trường hợp nào cố lợi dụng cơ chế bảo vệ "ấu trùng" nói trên. Ngoài ra, Czarnowski cũng dự đoán rằng công nghệ bảo vệ nhân hệ thống cho Vista mang tên PatchGuard sẽ trở thành mục tiêu lớn cho cộng đồng hacker bẻ phá. "Các kỹ thuật bẻ gãy hàng rào bảo vệ kernel có thể được chia sẻ công khai ngay trong năm

đầu tiên phát hành Vista, có khi còn sớm hơn cũng không chừng". Trọng Cầm