START MENU - "GÓT CHÂN ASIN" CỦA WINDOWS VISTA

Start

Start Menu chính là "gót chân Asin" của Windows Vista, tại đây cất giữ tất cả các chìa khóa để vào được "tòa lâu đài" Vista. Người đưa ra kết luận này là Robert Paveza, một chuyên gia phát triển các ứng dụng web của công ty marketing trực tuyến Terralever.

Paveza cũng là tác giả của phương pháp "tấn công 2 công đoạn" (two-stage attack) được thiết kế để tấn công Windows Vista bằng cách khai thác các điểm yếu ở User Account Control và thiết bị ảo hỗ trợ giao diện (shell) của hệ điều hành.

Kiểu tấn công này chủ yếu là dựa vào kỹ xảo "social engineering", một thủ thuật được nhiều hacker sử dụng cho các cuộc thâm nhập vào các hệ thống mạng, máy tính, nhằm "thả" một chương trình Trojan vào hệ thống. Giai đoạn đầu tập trung chủ yếu vào quá trình tương tác với người dùng và bố trí công cụ lây nhiễm qua proxy, một quá trình không đòi hỏi các đặc quyền quản trị. Nhiệm vụ cơ bản của công cụ lây nhiễm qua proxy, hay chính là Trojan, là mở ra giai đoạn tấn công thực sự nhằm gây hại cho Windows Vista.

"Giao diện Start Menu, cũng như desktop và bất kỳ phần nào khác của cấu trúc thư mục người dùng, đều có thể tiềm ẩn nguy cơ bị khai thác đối với người sử dụng. Như bạn thấy, trong tất cả các thư mục của người sử dụng - gồm Desktop, các phần của Start menu, thư mục Documents, Music, Video, Application Data - mỗi thư mục lại có thể được viết bởi người dùng sở hữu nó.

Ngoài ra, Start Menu tổng hợp All users (tất cả người dùng) và các thư mục Start Menu của một người dùng cụ thể được kết hợp, cùng với thư mục ưu tiên của người dùng, để tạo nên Start Menu hỗn hợp được biểu thị bởi trình tiện ích shell", Paveza mô tả.

Công cụ lây nhiễm qua proxy, hay Trojan, sẽ thay thế các shortcut từ desktop và thư mục Start Menu theo cách thức tương tự với cách thức của các virus đi kèm. "Công cụ lây nhiễm qua proxy, do người sử dụng điều khiển, sẽ ghi vào thư mục Start Menu của người sử dụng và đọc từ thư mục Start Menu toàn cầu mà không yêu cầu các phép nâng cao. Chương trình sẽ tìm trên thư mục Start menu toàn cầu tất cả các chương trình yêu cầu nâng cao và tạo ra các bản sao trong thư mục người dùng chỉ ra mã độc hại", Ron Bowes, chuyên gia nghiên cứu của hãng bảo mật Symantec cho biết.

Tất cả những gì chương trình độc hại này phải làm bây giờ là chờ người dùng chạy một trong số

các bản sao "dị hình" của các chương trình gốc chính thống trên bộ máy Windows Vista qua Start Menu hoặc desktop. Chỉ đến lúc này người dùng mới được trình diện với một yêu cầu nâng cao đặc quyền từ User Account Control, nhưng vì các chương trình gốc là "chính cống" nên các đặc quyền quản trị sẽ được công nhận ngay lập tức, nhờ thế mà cuộc tấn công gây hại cho hệ điều hành được hoàn tất.

Nguyễn Nam