TIN TẶC Ồ ẠT KHAI THÁC LỖI BẢO MẬT WINDOWS

Tin tặc ác ý hiện đang chủ động khai thác một lỗ hổng bảo mật nằm trong sản phẩm của Microsoft để "bắt cóc" đi nhiều hệ thống mắc lỗi phục vụ mục đích xây dựng mạng botnet. Các chuyên gia của hãng bảo mật Exploit Prevention Labs cảnh báo họ đã phát hiện ra m

Tin tặc ác ý hiện đang chủ động khai thác một lỗ hổng bảo mật nằm trong sản phẩm của Microsoft để "bắt cóc" đi nhiều hệ thống mắc lỗi phục vụ mục đích xây dựng mạng botnet. Các chuyên gia của hãng bảo mật Exploit Prevention Labs cảnh báo họ đã phát hiện ra một vài đoạn mã độc hại nhắm mục tiêu khai thác lỗi bảo mật phát sinh trong MDAC (Microsoft Data Access Components) để "gieo mầm mống" các hệ thống botnet. "Tôi đã phát hiện ra ít nhất 3 đoạn mã gieo mầm botnet trong tuần qua. Đây là một dấu hiệu cho thấy đã có ít nhất 3 nhóm tin tặc độc lập đã tự mình phát triển các công cụ khai thác lỗi bảo mật MDAC," Roger Thompson, kỹ sư công nghệ trưởng tại Exploit Prevention Labs, cho biết. "Theo những gì mà tôi biết, tính đến thời điểm này vẫn chưa có bất kỳ một đoạn mã nào được chứng minh là có khả năng khai thác lỗi bảo mật MDAC được công bố rộng rãi. Thông thường, tin tặc sẽ chỉ cần cắt-và-dán các đoạn mã đã được công bố vào trong công cụ khai thác riêng của chúng. Nhưng dường như trong trường hợp này chúng đã đảo ngược lại quá trình phát triển bản vá lỗi," Thompson nói. Lỗi bảo mật phát sinh trong MDAC đã được Microsoft khắc phục thông qua bản vá lỗi MS06-014 nằm phát hành trong bản cập nhật bảo mật tháng 4 là một lỗi cho phép thực thi đoạn mã từ xa. Lỗi này phát sinh trong ActiveX điều khiển RDS.Database - một phần của ActiveX Data Objects cấu thành nên MDAC. Một kẻ tấn công ác ý nếu khai thác thành công lỗi bảo mật này có thể chiếm toàn bộ quyền điều khiển hệ thống bị mắc lỗi. Trong vụ tấn công gần đây nhất, Thompson cho biết, người sử dụng Internet phải đứng trước nguy cơ bị tấn công nếu họ truy cập một trang web hoặc một thông điệp email "độc hại" có chứa một đoạn mã downloader cho phép tin tặc kiểm soát hệ thống của họ. "Một khi đoạn mã độc hại downloader được tải xuống, hệ thống của nạn nhân đã rơi vào tay của kẻ tấn công. Chúng sẽ đổ đầy hệ thống của nạn nhân bằng các phần mềm gián điệp và các chương trình chống spyware giả mạo. Chúng làm tất cả những điều đó chỉ vì mục đích kiếm tiền," Thompson cảnh báo. Hệ thống mạng thông minh của Exploit Prevention Labs đã phát hiện ra những đoạn mã có khả năng khai thác lỗi MDAC có liên quan đến bộ công cụ tự phát triển phần mềm gián điệp WebAttacker được rao bán trên một trang web của Nga với giá 300USD. Bộ công cụ này đã tích hợp sẵn các đoạn mã nhằm đơn giản hoá việc tấn công hệ thống mắc lỗi cũng các kỹ thuật gửi thư rác nhằm dụ dỗ nạn nhân truy cập vào các trang web độc hại sẵn có của chúng. Thompson cho biết việc xuất hiện đoạn mã khai thác lỗi MDAC là một mối đe doạ nghiêm trọng đối với người sử dụng Windows chưa cài đặt bản vá của Microsoft. Thompson khuyến cáo người sử dụng nên dùng tính năng Automatic Updates để nhanh chóng cài đặt các bản vá lỗi và bản cập nhật mới tránh trường hợp bị tấn công. Hoàng Dũng