ADOBE READER "CÕNG RẮN CẮN GÀ NHÀ"

Một chuyên gia nghiên cứu bảo mật người Anh vừa phát hiện ra một số phương thức sử dụng các tính năng của Adobe Reader để mở một cổng sau, tấn công các hệ thống PC. Mã khai thác và các tệp tin PDF được lập trình đặc biệt đã được chuyên gia David Kierznowsk

Một chuyên gia nghiên cứu bảo mật người Anh vừa phát hiện ra một số phương thức sử dụng các tính năng của Adobe Reader để mở một cổng sau, tấn công các hệ thống PC. Mã khai thác và các tệp tin PDF được lập trình đặc biệt đã được chuyên gia David Kierznowski công bố với mục tiêu minh chứng phương thức lợi dụng Adobe Reader để tấn công các hệ thống PC mà không cần bất kỳ một sự tương tác nào của người dùng. "Tôi không cho đây là một lỗi bảo mật trong ứng dụng PDF của Adobe. Đây chỉ là một cách bắt buộc những tính năng hợp pháp của ứng dụng thực hiện những công việc không có trong suy nghĩ của người đã thiết kế ra nó," Kierznowski khẳng định. Theo phương thức của Kierznowski, một liên kết độc hại sẽ được bổ sung vào trong tệp tin PDF. Nếu tệp tin đó được mở ra, trình duyệt của hệ thống sẽ tự động được khởi động và kết nối đến liên kết đó. "Như vậy tôi có thể khởi động bất kỳ một mã độc hại nào mà tôi muốn," Kierznowski cho biết. Phương thức sử dụng mã khai thác trên nền tảng web để khởi động một vụ tấn công "drive-by-malware download" là một hình thức khả phổ biến. Trong những vụ tấn công này các mã độc hại sẽ được khởi động và lây nhiễm lên hệ thống nạn nhân đồng thời tải thêm về nhiều mã độc hại khác. Bên cạnh đó, việc phát hiện "cổng sau" trên ứng dụng Adobe Reader minh chứng cho một sự thật là các ứng dụng trên máy tính để bàn đang trở thành một mục tiêu hấp dẫn bọn tội phạm mạng. Phương thức thứ hai lợi dụng Adobe Reader để mở một cổng sau trên hệ thống bị tấn công là sử dụng ADBC (Adobe Database Connectivity) của Adobe System và hệ thống dịch vụ web hỗ trợ Web Services. Phương thức này có thể dùng để tấn công cả những hệ thống Adobe Professional được vá lỗi đầy đủ. "Phương thức tấn công thứ hai cho phép kẻ tấn công có thể truy cập đến Windows ODBC, liệt kê các cơ sở dữ liệu hiện có và gửi những thông tin đó đi thông qua Web Services. Hình thức tấn công này có thể được phát triển thêm để thực hiện các lệnh điều khiển cơ sở dữ liệu thực sự. Bạn có thể tưởng tượng ra là nếu khai thác thành công một kẻ tấn công ác ý hoàn toàn có thể điều khiển cơ sở dữ liệu nội bộ của bạn thông qua trình duyệt web". Kierznowski tuyên bố hiện có ít nhất là hơn 7 điểm tồn tại trong các tệp tin PDF có thể bị tin tặc lợi dụng để kích hợp các mã độc hại. "Chỉ cần thêm một chút sáng tạo, kẻ tấn công có thể kết hợp các những phương thức tấn công đơn giản và phức tạp. Nguyên nhân có thể là do Adobe Acrobat hỗ trợ cả việc sử dụng HTML Form lẫn truy cập vào tệp tin hệ thống". "Một trong những phát hiện thú vị nhất của tôi là việc có thể dùng Adobe Acrobat để mở các cổng sau bằng cách kích hoạt một tệp tin JavaScript có chức năng mở cổng sau trong thư mục nằm trên hệ thống bị tấn công," Kierznowski cho biết. Người phát ngôn của Adobe cho biết hiện hãng này đang tiến hành điều tra vấn đề mà Kierznowski vừa phát hiện ra. Hoàng Dũng