MINH CHỨNG CHO SỰ ĐỘC HẠI CỦA JAVACRIPT

Một ch

Một chuyên gia nghiên cứu bảo mật vừa phát hiện được cách mà tin tặc biến một chiếc PC thành công cụ phục vụ mục đích đen tối của chúng mà không cần phải "bắt cóc".

Đó là điều mà Jikto - một công cụ bảo mật mới của chuyên gia nghiên cứu bảo mật Billy Hoffman của SPI Dynamics - làm được. Công cụ được lập trình bằng ngôn ngữ Javascript này có thể biến PC thành công cụ săn lùng lỗi bảo mật web mà người chủ sở hữu của nó không hề hay biết.

Dự kiến Hoffman sẽ công bố công cụ Jikto tại diễn đàn ShmooCon Hacker vào cuối tuần này.

"Công cụ này sẽ thay đổi suy nghĩ của chúng ta về những gì mà tin tặc có thể làm được với Javascript," Hoffman khẳng định. "Jikto có thể biến bất kỳ PC nào thành công cụ săn tìm bảo mật hoặc tấn công website khác."

Thực chất Jikito là một ứng dụng quét lỗi bảo mật website. Ứng dụng này bí mật quét kiểm tra các trang web và trả về kết quả. Jikto có thể được nhúng vào bất kỳ trang web nào - website của tin tặc hoặc website hợp pháp - bằng cách khai thác lỗ hổng XSS (cross-site scripting).

Jikto có thể săn lùng và phát hiện được hầu hết các lỗ hổng bảo mật web thường thấy hoặc có thể săn lùng lỗ hổng web theo yêu cầu. Ví dụ Jikto có thể chỉ săn lùng lỗ hổng SQL Injection trong các trang web ngân hàng trực tuyến chẳng hạn.

Bởi vì Jikto được lập trình bằng Javascript nên công cụ này có thể vận hành trên hầu hết các loại trình duyệt mà không hề đưa ra bất kỳ cảnh báo nào cho người dùng. Người dùng Internet có thể chạm mặt với một website có nhúng Jikto trên Internet mà không hề biết. Công cụ này sẽ hoạt động chừng nào cửa sổ trình duyệt còn đang mở và biến mất không để lại bất kỳ một dấu vết nào khi cửa sổ trình duyệt đóng lại.

Hiện Hoffman đang nghiên cứu phát triển phiên bản Jikto kế tiếp có khả năng khai thác lỗi bảo mật và lấy dữ liệu. Dự kiến phiên bản này sẽ được trình diễn tại Black Hat vào mùa hè năm nay.

Hoàng Dũng