JAVASCRIPT - CÔNG CỤ TẤN CÔNG CỰC KỲ NGUY HIỂM

Các chuyên gia bảo mật vừa phát hiện được một phương thức sử dụng JavaScript để vẽ bản đồ hệ thống mạng gia đình hoặc doanh nghiệp và tấn công vào các máy chủ, thiết bị có thể kết nối được. Các đoan mã JavaScript độc hại có thể được nhúng vào tron

Các chuyên gia bảo mật vừa phát hiện được một phương thức sử dụng JavaScript để vẽ bản đồ hệ thống mạng gia đình hoặc doanh nghiệp và tấn công vào các máy chủ, thiết bị có thể kết nối được. Các đoan mã JavaScript độc hại có thể được nhúng vào trong một trang web. Mỗi khi trang web này được duyệt trong các loại trình duyệt, đoạn mã đó sẽ âm thầm chạy mà không hề đưa ra các cảnh báo cho người dùng. Các chuyên gia nghiên cứu cho biết những loại đoạn mã độc hại nói trên hoàn toàn có thể vượt qua mọi ứng dụng tường lửa vì nó được thực thi thông qua trình duyệt web - ứng dụng hoàn toàn hợp pháp trước con mắt của ứng dụng tường lửa. "Chúng tôi đã tìm ra được một kỹ thuật để quét toàn bộ một hệ thống mạng và xác định mọi thiết bị có khả năng web. Kỹ thuật đó còn cho phép chúng tôi gửi các lệnh hoặc tấn công luôn những thiết bị đó," Billy Hoffman - một kỹ sư hàng đầu của SPI Dynamics - cho biết. "Kỹ thuật này còn có thể quét cả các hệ thống mạng được bảo vệ bằng tường lửa - như hệ thống mạng của các doanh nghiệp chẳng hạn." Nếu một vụ tấn công sử dụng kỹ thuật nói trên thành công thì nó có thể gây ra những ảnh hưởng tác hại đáng kể. Lấy ví dụ, vụ tấn công đó quét hệ thống mạng gia đình của người dùng, phát hiện một loại sản phẩm bộ định tuyến mạng (router), gửi các lệnh để kích hợp tính năng mạng không dây đồng thời tắt mọi tính năng mã hoá. Hoặc một hệ thống mạng doanh nghiệp có thể sẽ bị lập bản đồ chi tiết và bị tấn công. Tuy nhiên, những vụ tấn công đó nếu bị phát hiện nó lại có vẻ như là vụ tấn công được thực hiện từ chính trong mạng nội bộ của công ty đó. "Trình duyệt của bạn hoàn toàn có thể được sử dụng để tấn công vào hệ thống mạng nội bộ," Jeremiah Grossman - kỹ sư công nghệ trưởng của WhiteHat Security - khẳng định. Cả SPI Dynamics và WhiteHat Security đều phát hiện được kỹ thuật tấn công bằng JavaScript nói trên cùng một lúc với nhau. Dự kiến hai hãng sẽ cùng công bố kỹ thuật này tại Hội nghị Black Hat sẽ được tổ chức trong tuần tới. Vẫn còn bỏ ngỏ? JavaScript đã được ứng dụng trên web trong khoảng một thập kỷ qua. Ngôn ngữ lập trình kịch bản được chủ yếu ứng dụng trên các trang web và đang ngày càng trở nên phổ biến nhờ vào một kỹ thuật lập trình có tên là AJAX (JavaScipt và XML không đồng bộ). Kỹ thuật AJAX giúp tăng tính tương tác của các trang web nhưng cũng có những hiểm hoạ bảo mật tương tự như JavaScript. Trong khi đó, các đoạn mã JavaScript độc hại cũng đã được biết đến từ lâu nhưng các chuyên gia bảo mật lại ít quan tâm đến nó, Fyodor Vaskovich - người sáng tạo nên công cụ quét cổng, săn lỗi Nmap nổi tiếng - cho biết. "Thường những vụ tấn công kiểu như đề cập ở trên rất ít được quan tâm đến," Vaskovich nói. "Nhưng một vấn đề mấu chốt trong lỗi bảo mật được SPI Dynamics phát hiện là lỗi bảo mật đó rất khó có thể khắc phục. Khắc phục nó có thể sẽ làm hỏng các ứng dụng web. Chính vì thế có lẽ chúng ta cần có nhiều năm nữa mới có thể khắc phục được". Đã từng có nhiều nỗ lực nhằm lập trình một công cụ quét mạng bằng JavaScript. Nhưng chưa có một công cụ nào tiên tiến như ví dụ mà SPI Dynamics đưa ra, Vaskovich khẳng định. "SPI Dynamics xứng đáng được khen ngợi khi phát hiện ra kỹ thuật tấn công nói trên." Chưa có giải pháp khắc phục Khi vận hành, đoạn mã JavaScript độc hại trước hết sẽ xác định địa chỉ nội bộ của PC. Sau đó sẽ sử dụng các lệnh và đối tượng chuẩn của JavaScript để tiến hành quét mạng nội bộ tìm các máy chủ web. Đó có thể thực sự là các máy chủ web hoặc các thiết bị như router, máy in, điện thoại IP hoặc các thiết bị, ứng dụng mạng khác có giao diện điều khiển web. Đoạn mã JavaScipt sẽ tiếp tục xác định xem PC có địa chỉ IP hay không bằng cách gửi một lệnh

"PING" thông qua đối tượng "IMAGINE" của JavaScript. Bước kế tiếp là nó sẽ xác định các loại máy chủ nào đang chạy bằng cách tìm kiếm các tệp tin ảnh thường được lưu trong các thư mục chuẩn. Một đoạn mã JavaScript độc hại có thể được lưu trữ trên trang web của kẻ tấn công. Một cuộc tấn công như thế này có thể núp bóng dưới các trang web đáng tin cậy nhờ vào việc khai thác lỗi tấn công kịch bản liên trang (cross-site scripting). Những công ty có tên tuổi như Google, Microsoft hay eBay đã từng phải bỏ nhiều công sức để khắc phục những lỗi bảo mật đó. Mới đầu tuần này, Nestcape cũng đã phải khắc phục một lỗi bảo mật tương tự. Với kỹ thuật tấn công kiểu này thì sẽ có rất ít người dùng cá nhân có thể được bảo vệ. Gánh nặng giờ đây đã đổ lên vai các nhà phát triển web nhằm bảo đảm an toàn cho người dùng và máy chủ web. Một số phần mềm bảo mật có khả năng phát hiện được các đoạn mã JavaScript độc hại nhưng chỉ là đoạn mã được sử dụng trong các vụ tấn công trên bề mặt. Còn tấn công theo kiểu ngầm như trên chắc ứng dụng đó cũng chịu thua. Khuyến cáo được đưa ra đối với những người quản trị máy chủ. Các nhà quản trị máy chủ và trang web nên khắc phục mọi lỗi tấn công kịch bản liên trang và tiến hành chứng thực JavaScript người dùng. Còn người dùng nên vô hiệu hoá tính năng JavaScript của trình duyệt. Hoàng Dũng