'COOKIE ĐỘNG' - GIẢI PHÁP BẢO MẬT CHỐNG LỪA ĐẢO MỚI

Các nhà khoa học thuộc trường ĐH công nghệ thông tin bang Indiana Mỹ đã phát triển thành công một kĩ thuật bảo mật mới mang lại khả năng bảo vệ mạnh mẽ hơn chống lại các cuộc tấn công điện tử và tội phạm mạng. Chuyên gia bảo mật điện tử Markus Jakobsson và RavenWh

Các nhà khoa học thuộc trường ĐH công nghệ thông tin bang Indiana Mỹ đã phát triển thành công một kĩ thuật bảo mật mới mang lại khả năng bảo vệ mạnh mẽ hơn chống lại các cuộc tấn công điện tử và tội phạm mạng. Chuyên gia bảo mật điện tử Markus Jakobsson và RavenWhite - một công ty mới thành lập trong đó Jakobsson là một thành viên sáng lập - đã phát triển thành công "cookie động". Đây là một giải pháp bảo mật mới được thiết kế nhằm chống lại tấn công lừa đảo trực tuyến như pharming hay ăn cắp thông tin cá nhân. "Hiện vẫn chưa có bất kì một công cụ thương mại đáng tin cậy nào để bảo vệ người dùng khỏi những cuộc tấn công như vậy," Jakobsson nói. "Chúng tôi tin tưởng rằng 'cookie động' có thể làm được điều đó." 'Cookie động' có thể được ứng dụng trong một số trường hợp mà cookie truyền thống không thể thực hiện đúng chức năng của mình. Phát minh của Jakobsson không những có thể giúp chúng ta bảo vệ tránh khỏi những kiểu tấn công lừa đảo trực tuyến hay ăn cắp thông tin cá nhân đã được biết đến mà còn các những mối đe dọa tấn công mới tương tự như các vụ tấn công do Mark Meiss và Alex Tsow - hai sinh viên bảo vệ học vị tiến sĩ tin học tại trường ĐH công nghệ thông tin bang Indiana - phát hiện ra. Trong đó Meiss phát hiện ra một kĩ thuật cho phép kẻ tấn công ác ý đột nhập vào hầu hết các kết nối Wi-Fi nhằm phục vụ mục đích chuyển hướng người dùng sang một trang web hoàn toàn khác với trang web mà họ muốn truy cập. Meiss cũng đã chứng minh tính thực tế của kĩ thuật này tại một điểm hotspot gần nơin toảnsống. "Không có một giải pháp cụ thể nào giúp người dùng có thể nhận biết được các vụ tấn công đang diễn ra," Meiss giải thích. "Bạn có thể không chắc chắn là mình đang truy cập trang web ngân hàng nơi bạn gửi tiền mặc dù trang web đó nhìn có vẻ giống. Không có một cách nào giúp chúng ta phân biệt được." Trong khi đó Tsow phát hiện ra các bộ định hướng người dùng cũng có thể bị lợi dụng để chuyển hướng người dùng sang một trang web khác với trang web mà người dùng muốn truy cập. Tsow đã chứng minh kĩ thuật này bằng cách mở trình duyệt nhập địa chỉ của eBay nhưng trình duyệt lại trả lại trang web của Anti-Phishing Working Group. "Trong vụ tấn công thực tế người dùng sẽ bị chuyển đến một trang web giống hệt với trang web mà họ muốn vào thăm. Nhưng chắc chắn trang web đó được vận hành bởi các kẻ tấn công ác ý nhằm ăn cắp tên đăng nhập hay mật khẩu tài khoản ngân hàng của người dùng," Tsow nói. Jakobsson cho rằng 'cookie động' hoàn toàn có thể bảo vệ người dùng tránh khỏi những cuộc tấn công kể trê hay các cuộc tấn công giả mạo tên miền ... nhằm phục vụ cho mục đích lừa đảo trực tuyến. RavenWhite cho rằng các công nghệ cơ bản sẽ không có khả năng bảo vệ người dùng cuối cùng do vậy mà công ty này đang phát triển các công nghệ máy chủ nhằm chống lại các cuộc tấn công ngày càng phức tạp. Để tìm hiểu thêm về công nghệ mới của RavenWhite bạn có thể tham khảo thêm tài liệu tại đây.