TROJAN GIẢ MẠO FIREFOX ADD-ON CỰC KỲ NGUY HIỂM

Hãng bảo mật McAfee hôm qua đã phát hiện một con trojan giả mạo như là một ứng dụng bổ sung (add-on) cho trình duyệt Firefox nhằm đột nhập vào hệ thống của người dùng. Keylogg cả chuột và bàn phím Trên thực tế, con trojan FormSpy là một con keylogger có

Hãng bảo mật McAfee hôm qua đã phát hiện một con trojan giả mạo như là một ứng dụng bổ sung (add-on) cho trình duyệt Firefox nhằm đột nhập vào hệ thống của người dùng. Keylogg cả chuột và bàn phím Trên thực tế, con trojan FormSpy là một con keylogger có chức năng giám sát mọi hoạt động của con trỏ chuột và bàn phím nhằm ăn cắp thông tin cá nhân của người dùng như thông tin đăng nhập tài khoản ngân hàng trực tuyến, liên kết URL trong trình duyệt Firefox ... Không những thế con trojan này còn có khả năng ăn cắp mật khẩu từ các ứng dụng khác như ICQ, FTP, giao thông thư điện tử IMAP và POP3, hãng bảo mật McAfee cho biết. Mọi thông tin thu thập sẽ được con trojan gửi về địa chỉ IP của kẻ tấn công. Cực kỳ tinh vi Con trojan này là một phần trong chiến dịch lừa đảo qua email với các thông điệp điện tử được gửi đi từ văn phòng hỗ trợ thanh toán của hãng bán lẻ nổi tiếng toàn cầu Wal-Mart, Craig Schmugar - một chuyên gia nghiên của của McAfee - cho biết. "Các email được gửi đi trong chiến dịch lừa đảo này đều có chứa mã số đơn đặt hàng chính vì thế mà người dùng rất dễ mở các email đó ra. Nếu những email đó được mở ra, con trojan sẽ đột nhập vào hệ thống và cài đặt thêm hai bộ phận khác của chúng - trong đó có một con keylogger." Tuy nhiên, cách thức mà con trojan FormSpy phát tán và đột nhập vào hệ thống cũng rất khác biệt - cách thức này có thể nói là độc nhất vô nhị tại thời điểm này, Schmugar nói. Con trojan này giả mạo như là một ứng dụng bổ sung cho trình duyệt mã nguồn mở Firefox. Thực tế FormSpy giả mạo là ứng dụng bổ sung Numberedlinks 0.9 - một ứng dụng bổ sung cho phép người dùng có thể truy cập các liên kết bằng bàn phím. FormSpy cũng sử dụng một số đoạn mã của Numberedlinks để tích hợp hoàn toàn vào trong Firefox. Thông thường, một ứng dụng bổ sung cho Firefox trên nền tảng Windows thường hiển thị một hộp thoại cho phép người dùng khẳng định là có cài đặt hay không. Tuy nhiên, con trojan FormSpy đã bỏ qua bước đó. Con trojan này ghi đè mọi thông itn lên thư mục Firefox mà không hề cảnh báo người dùng. Người dùng bị nhiễm mà không hề biết là do một ứng dụng bổ sung mở rộng làm nên. Thậm trí trình duyệt Firefox còn xác nhận ứng dụng bổ sung lừa đảo này như một ứng dụng bổ sung hợp pháp và hiển thị danh sách khi truy cập vào Tools | Extensions. Bổ sung ư? Quá mất an toàn Các ứng dụng bổ sung của Firefox từ lâu đã được xem là rất kém tính an toàn, đặc biệt là khi chúng không có chứng thực kỹ thuật số. Sự giả mạo của FormSpy sẽ thêm một lần nữa làm sống lại vấn đề này. "Con trojan đã sử dụng một cơ chế để đưa các đoạn mã của nó xâm nhập vào trình duyệt," Schmugar nói. "Mozilla nên cân nhắc nhiều hơn nữa đến tính bảo mật của các ứng dụng bổ sung". Hoàng Dũng