Người dùng Google Chrome đang gặp nguy

Hàng chục triệu máy tính sử dụng Google Chrome đang gặp nguy hiểm vì cài tiện ích mở rộng (extension) chứa mã độc.

Các nhà nghiên cứu bảo mật từ Awake Security ngày 18/6 tuyên bố phát hiện phần mềm gián điệp (spyware) ẩn trong các extension trên trình duyệt Google Chrome với hơn 32 triệu lượt tải, được phát hành trên kho ứng dụng Chrome Web Store.
Theo *CNN*, ít nhất 111 extension độc hại hoặc giả mạo được phát hiện có khả năng chụp ảnh màn hình, đánh cắp thông tin đăng nhập. Một số hệ thống tài chính, y tế và tổ chức chính phủ đã bị ảnh hưởng.

Lỗ hổng kiểm duyệt của Google Chrome đã để lọt hơn 100 extension chứa phần mềm gián điệp xuất hiện trên kho ứng dụng Chrome Web Store. Ảnh: *Threat Post*.

Sau khi được các tổ chức bảo mật cảnh báo hồi tháng trước, Google đã gỡ các extension chứa phần mềm độc hại khỏi Chrome Web Store.

Scott Westover, phát ngôn viên Google nói với *Reuters* rằng công ty sẽ dùng các extension này để cải thiện bộ phận phân tích, kiểm duyệt extension trong tương lai.

Đa số extension chứa phần mềm độc hại được phát hành miễn phí, núp bóng dưới dạng trình chuyển định dạng tập tin hoặc cảnh báo một website có dấu hiệu không an toàn. Tuy nhiên khi cài đặt xong, chúng sẽ thu thập lịch sử duyệt web và thông tin đăng nhập của người dùng.

Dựa trên lượt tải các extension độc hại, đây được xem là "chiến dịch tấn công người dùng Google Chrome bằng phần mềm độc hại lớn nhất từ trước đến nay" theo Gary Golomb, đồng sáng lập Awake Security.

Tuy xác nhận sự tồn tại của extension chứa phần mềm gián điệp, Google không nói rõ quy mô cuộc tấn công, mức độ thiệt hại hoặc tại sao chỉ xử lý khi được các hãng bảo mật cảnh báo. Ngoài ra, cũng chưa rõ tổ chức hoặc cá nhân nào đứng sau vụ việc bởi các lập trình viên đã nhập thông tin giả khi phát hành extension.

Ben Johnson, cựu kỹ sư Cơ quan An ninh Quốc gia Mỹ nhận định bất cứ thứ gì cho phép truy cập vào trình duyệt, email hoặc thông tin nhạy cảm của người khác đều có thể là mục tiêu của các hoạt động gián điệp quốc gia hoặc tội phạm có tổ chức.

Trình duyệt web phổ biến nhất thế giới liên tục gặp những vấn đề nghiêm trọng thời gian gần đây. Ảnh: *Reuters*.

Theo Golomb, những extension độc hại này được thiết kế tránh bị các trình diệt virus phát hiện. Khi trình duyệt được sử dụng, nó sẽ kết nối với hàng loạt website khác để

truyền thông tin, thậm chí xâm nhập vào mạng máy tính gia đình hoặc doanh nghiệp mà người dùng không hề biết.

Các nhà nghiên cứu từ Awake đã phân tích một extension và nhận thấy bên trong chứa 15.000 tên miền liên kết với nhau, được mua từ một công ty có tên Galcomm của Israel.

Trả lời *Reuters*, Moshe Fogel, chủ sở hữu Galcomm cho biết: "Công ty chúng tôi không liên quan hoặc hợp tác với bất cứ hoạt động độc hại nào. Ngược lại, chúng tôi hợp tác với các cơ quan chức năng để ngăn chặn hoạt động phi pháp".

Sau khi nhận danh sách tên miền, Fogel cho biết đa số chúng không hoạt động nhưng sẽ tiếp tục điều tra những tên miền khác.

Phần mềm độc hại trong extension trình duyệt là thủ đoạn tấn công không hề mới, tuy nhiên tác hại của chúng ngày càng lớn. Từ hiển thị quảng cáo, những extension sau này còn có thể theo dõi hành vi, thu thập dữ liệu trái phép.

Các lập trình viên đã tận dụng Chrome Web Store để phát hành extension độc hại trong thời gian dài. Vào năm 2018, Google cho biết sẽ tăng cường kiểm duyệt các extension bằng cách sử dụng con người để kiểm duyệt.

Tuy nhiên vào tháng 2 vừa qua, nhà nghiên cứu Jamila Kaya và đội ngũ Duo Security của Cisco phát hiện một số extension độc hại trên Chrome đã đánh cắp dữ liệu của 1,7 triệu người dùng. Sau khi điều tra, Google phát hiện và gỡ bỏ khoảng 500 extension bị cài mã độc.

Phúc Thịnh (Theo Reuters) trang https://zingnews.vn/