HACKER CÓ THỂ KIỂM SOÁT MÁY TÍNH QUA ADD-ON CỦA FIREFOX

Nh

Những kẻ tấn công có thể nguy trang malware như một phần mở rộng của Firefox

Một số chuyên gia bảo mật mới đây đã công bố rằng: Hacker có thể "thả" đoạn mã độc hại vào hệ thống chạy Firefox của Mozilla khi trình duyệt này sử dụng thêm một vài add-on, bao gồm cả Google Toolbar và Yahoo Toolbar. Mozilla đã thừa nhận nguy cơ kiểu này trên một vài tính năng mở rộng.

Christopher Soghoian, một nghiên cứu sinh Ph.D. tại trường đại học Indiana, đã phác thảo qua phương thức "man-in-the-middle"mà kẻ tấn công có thể sử dụng, đặc biệt là trong các mạng không dây công cộng. Kẻ tấn công có thể ngụy trang malware như một phần mở rộng của Firefox và lén gài mã độc hại vào thay vì cập nhật thông thường cho một trong những phần mở rộng bị hổng.

Các gói mở rộng của Firefox - thường là các gói nhỏ nhằm thêm tính năng cho Firefox, chúng gần như được tạo phổ biến bởi những nhà phát triển tình nguyện hoặc theo sở thích – được lưu trữ và cập nhật tại trang được bảo mật SSL của chính Mozilla và không được phòng bị trước kiểu tấn công này, Soghoian nói. Đa phần trong số gói mở rộng đó được tạo bởi bên thứ ba, tuy nhiên việc cập nhật lại từ trên các máy chủ không đảm bảo của họ.

"Đây có thể xem là một lỗi kép. Mozilla không nói với các nhà phát triển là họ nên cập nhật từ một đường liên kết an toàn; họ sai lầm khi cho rằng tất cả mọi người đều biết điều đó. Nhưng các nhà phát triển phần add-on đó cũng gặp khiếm khuyết khi không sử dụng máy chủ bảo mật", Soghoian nói.

Sau khi nhận được cảnh báo của Soghoian, Mozilla đã chỉnh sửa tài liệu hướng dẫn bảo trì và cập nhật ứng dụng mở rộng Firefox. Họ đã thúc đẩy các nhà phát triển nâng cấp máy chủ lên kết nối an toàn SSL.

Các điểm truy cập mạng không dây công cộng (như ở sân bay hay quán cà phê) là nơi phần lớn xảy ra các cuộc tấn công, bởi vì hacker có thể truy cập chúng một cách dễ dàng và giả dạng như một máy chủ cập nhật hợp pháp chỉ với một chiếc máy tính xách tay. Nhưng Soghoian đã cảnh báo rằng một số mạng khác cũng nguy hiểm không kém.

“Bất kể mạng ở nơi đâu bạn cũng không nên đặt mình vào thế nguy hiểm. Ví dụ như sử dụng mạng không dây của hàng xóm.” Người dùng trong mạng nặc danh Tor cũng có thể bị nguy hiểm, Soghoian nói thêm. “Đó là những nơi bạn có thể ‘giao” DNS của mình cho một số người mà bạn không hề biết”

Google Toolbar, Yahoo Toolbar, Del.icio.us Extension, Facebook Toolbar, AOL Toolbar, Ask.com Toolbar, Netcraft Anti-Phishing Toolbar và PhishTank SiteChecker cũng nằm trong số các add-on nguy hiểm, và Soghoian còn chưa liệt kê hết được danh sách đó. “Tôi không có thời gian để kiểm tra toàn bộ các phần mở rộng đó, vì vậy tôi đã vào Download.com và tìm kiếm ở top 20”. Soghoian cũng khuyên rằng trước khi các hãng cung cấp phần mở rộng đưa ra phần cập nhật bảo mật, người dùng nên gỡ bỏ hoặc vô hiệu hóa toàn bộ tính năng mở rộng cũng như toolbar của Firefox mà không trực tiếp download từ trên website Add-Ons của Mozilla.

Mike Shaver – lãnh đạo Mozilla cũng đã thừa nhận nguy hiểm không an toàn cho việc lưu trữ và cập nhật add-on, ông cũng đề xuất các nhà phát triển phần mở rộng nên nhanh chóng giải quyết vấn đề.

Hồng Ngân