NHỮNG DẤU HIỆU NGUY HIỂM NÊN TRÁNH KHI LƯỚT WEB

Tội ph

Tội phạm mạng thường xuyên thay đổi chiến thuật hòng thâm nhập vào các hệ thống máy tính, do đó người sử dụng cần cảnh giác ngay cả trong những trường hợp tưởng như vô hại.
E-mail giả danh ngân hàng, trang đấu giá trực tuyến hay tổ chức có uy tín nào đó... để yêu cầu người sử dụng bấm vào đường link hoặc tải tài liệu đính kèm chứa mã độc. Trong ảnh là một thông điệp giả mạo tổ chức BBB (Ảnh: SecureWorks):

Nếu nhận được tài liệu Word đính kèm và thấy yêu cầu "click đúp chuột để xem chi tiết tài liệu" thì nên xóa file ngay lập tức (Ảnh: PC World):

Thông báo giả Automatic Updates, được phát hiện trên một hồ sơ MySpace, khẳng định hệ thống của người dùng bị nhiễm virus và yêu cầu cài công cụ gỡ bỏ phần mềm nguy hiểm (Ảnh: FaceTime Security Labs):

Bước tiếp theo của quá trình tấn công bằng Automatic Updates này là gây cho người dùng nỗi hoang mang rằng hệ thống của mình đã bị nhiễm độc. Thông qua đó đưa ra thông báo hỗ trợ để người dùng cả tin có thể kích vào (Ảnh: FaceTime Security Labs):

Những kẻ phát tán spyware thường đăng video có tựa đề hấp dẫn để lôi kéo người sử dụng. Khi bấm vào, họ sẽ thấy thông báo rằng cần tải codec thì mới xem được clip. Nếu thực hiện theo, cái mà người dùng nhận được không phải đoạn phim mát mẻ mà là phần mềm gián điệp Zlob (Ảnh: Sunbelt Software):

Bạn có nghĩ đây là malware độc hại? Thậm chí cuộc tấn công bằng cách cài đặt mã codec này còn 'siêu' hơn ở chỗ hiển thị một giao diện xác nhận đồng ý bản quyền trong quá trình cài đặt (Ảnh: Sunbelt Software):

Hacker thường tạo ra những trang web độc có URL bắt đầu bằng tên website nổi tiếng (chẳng hạn

PayPal.com) nhưng phần đuôi lại được kéo dài bằng những ký tự vô nghĩa logwjwgwwwqwkqwk.com:

Nếu thấy nghi ngờ một file nào đó, hãy tải nó lên trang Virustotal.com, nơi hỗ trợ hơn 30 công cụ quét virus khác nhau để kiểm tra: