PANDA: CẨN THẬN VỚI ADWARE "GIÁN ĐIỆP"

Hãng b

Hãng bảo mật Panda Software vừa phát hiện một loại phần mềm quảng cáo (adware) cực kỳ nguy hiểm có thể cho phép tin tặc theo dõi tiến trình duyệt web của người dùng.

Adware nói trên lây nhiễm vào PC của người dùng khi họ truy cập vào các website giả mạo cung cấp nội dung người lớn do tin tặc điều khiển.

Phương thức đột nhập của adware này như sau: Nó giả mạo một ActiveX Control có tên là ImageAccesActiveXObject đưa ra thông báo đề nghị người dùng phải cài đặt thì mới xem được bức ảnh mà họ vừa nhấp chuột vào.

Đồng ý cài đặt ActiveX Control đồng nghĩa với việc người dùng tạo điều kiện cho adware được phép cài đặt lên hệ thống. Để tránh sự chú ý của người dùng khi cài đặt xong nó cũng đưa ra thông báo ActiveX đã cài đặt thành công và hiển thị bức ảnh cho người xem.

Người dùng có thể tham khảo phương thức lây nhiễm qua một video do Panda đưa lên làm minh chứng.

"Trước đây chúng tôi mới chỉ phát hiện được dạng adware giả mạo codec video chứ chưa từng diện kiến adware giả mạo ActiveX Control phục vụ xem ảnh. Đây là một thủ đoạn lừa người dùng mới của tin tặc. Chúng khiến người dùng tưởng lầm là họ đang cài đặt một công cụ hợp pháp," ông Luis Corrons - Giám đốc kỹ thuật của PandaLabs - cho biết.

Khi đã cài đặt thành công adware sẽ được người dùng đến một trang chứa đầy các bức ảnh khiêu dâm. Trong khi đó nó lại tải thêm về nhiều mã độc hơn về PC bị nhiễm. Mục tiêu chính là cho phép tin tặc theo dõi mọi hoạt động trên Internet của người dùng PC bị nhiễm.

Hoàng Dũng