

VIRUS NGẤM BẮN VIDEO CLIP

Sự bùn

Sự bùng nổ của trào lưu video clip "cây nhà lá vườn" đã khiến hacker và giới tội phạm mạng không thể làm ngơ.

Các hãng bảo mật vừa ghi nhận được một số codec Windows "trá hình" - hay các phần mềm nén file - trong khi cho phép người dùng xem video clip đã ngấm ngầm cài đặt spyware và adware vào máy tính.

Một số site như YouTube sử dụng các công nghệ rất ưu việt, cho phép xem video clip qua mạng không hề khó khăn, nhưng cũng có không ít site khác đòi hỏi người dùng phải cài đặt thêm phần mềm (gọi là codec) thì mới xem được.

Nguồn: AP

Lợi dụng khe hở này, hacker đã tìm cách chèn thêm vào những codec thông dụng một dãy spyware và adware. Một số codec cũng giúp người dùng xem clip thật, nhưng đại đa số chỉ dùng codec để ngụy trang mà thôi.

Ngay khi hạ cánh xuống máy tính, chúng sẽ hoạt động cần mẫn như một malware thực thụ. Có thể là đội bom người dùng với những quảng cáo pop-up, mà cũng có thể là lén lút chạy chương trình theo dõi bàn phím, cố gắng ăn cắp thông tin nhạy cảm của bạn.

Tình quái hơn, phần mềm codec mà hãng Sunbelt Software phát hiện được còn "phát minh" ra những lỗi bảo mật không hề tồn tại bên trong máy tính và yêu cầu người dùng trả tiền để ... khắc phục.

Nguy hiểm nhất là khi bị các công cụ diệt virus scan, các codec này đều tỏ ra rất "vô tội". Nhưng chỉ cần cài đặt xong xuôi, chúng sẽ móc nối ngay với website chủ và tải bản update về máy.

Ông Robinson cho rằng sự nổi lên của những phần mềm giải nén video clip là một thí dụ nữa minh chứng cho việc tội phạm mạng đã trưởng thành và tiến hóa vượt bậc so với ngày xưa, thời virus chỉ có mỗi con đường "du hành độc đạo" là thông qua email.

"Giờ đây, bọn chúng sở hữu một danh sách dài các kỹ xảo tấn công và chỉ cần chỉnh sửa đôi chút cho phù hợp với những xu hướng đáng "nóng", mốt là được".

Đồng tình với nhận định này, chuyên gia David Emm của hãng bảo mật Kaspersky cho rằng việc hacker quay sang khai thác những site như YouTube chỉ còn là vấn đề thời gian. "Rồi các video clip sẽ lỗ chỗ toàn malware và lỗ hổng", Emm dự đoán.

Trọng Cẩm