BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 683/CATTT-TĐQLGS
V/v biện pháp phòng, chống mã độc lây lan thông qua Facebook Messenger tại Việt Nam

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 19 tháng 12 năm 2017

Kính gửi: - Đơn vị chuyên trách về CNTT các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; Các Ngân hàng TMCP; Các tổ chức tài chính.

Sáng 19/12/2017, nhiều người dùng sử dụng ứng dụng Facebook Messenger tại Việt Nam đã trở thành nạn nhân của một loại mã độc được cho là sử dụng để đào tiền ảo. Mã độc này lây lan bằng cách gửi đi một tập tin tên là video_xxx.zip (trong đó xxx là các số ngẫu nhiên). Đây là một tập tin nén trong đó có chứa tập tin với định dạng mp4.exe, thực chất là tập tin thực thi của hệ điều hành Windows. Tuy nhiên người dùng thông thường lại nhầm tưởng là tập tin Video (mp4) nên dễ dàng tin tưởng mở tập tin.

Qua phân tích kỹ thuật ban đầu của Cục An toàn thông tin, loại mã độc này khi lây nhiễm vào máy tính người dùng sẽ thực hiện những hoạt động sau:

Mã độc tự động tải và cài đặt một số tập tin độc hại: 7za.exe, files.7z từ trang web độc hại có tên miền yumuy.johet.bid (với các mẫu mã độc khác nhau, tên miền này có thể thay đổi).

Mã độc sẽ sử dụng tập tin 7za.exe để giải nén tập tin file.7z, sau đó lấy tiện ích mở rộng (extension) độc hại và tự động cài đặt tiện ích mở rộng này này vào trình duyệt Chrome. Đồng thời, mã độc này không cho người dùng truy cập vào phần quản lý tiện ích mở rộng của trình duyệt. Trong tập tin được giải nén có chứa các tập tin thực thi được cho là sử dụng nhằm mục đích lợi dụng tài nguyên máy tính người dùng để đào tiền ảo.

Thông qua các biện pháp kỹ thuật xác định được tác giả của mẫu mã độc này có thể đang sử dụng địa chỉ email có tên miền là *kadirgun.com*.

Theo các chuyên gia an toàn thông tin, những người dùng trình duyệt Chrome là đối tượng chính của mẫu mã độc này. Không loại trừ khả năng trong thời gian tới sẽ xuất hiện các mẫu mã độc nhằm vào các trình duyệt khác.

Nhằm bảo đảm an toàn thông tin và phòng tránh nguy cơ bị tấn công bởi mã độc, Cục An toàn thông tin khuyến nghị:

- Cảnh giác và không mở các tập tin hay đường dẫn lạ được gửi qua Facebook Messenger hay bất kỳ ứng dụng truyền thông nào khác (ví dụ: Viber, Zalo, thư điện tử, …).

- Nếu nhận được các thông tin (tập tin hoặc đường dẫn) lạ, có thể thông báo hoặc gửi thông tin về Cục An toàn thông tin để tổng hợp và phân tích, cảnh báo khi có những dấu hiệu, nguy cơ tấn công mạng mới.

- Đối với người dùng đã bị lây nhiễm cần cài đặt và cập nhật các phần mềm phòng, chống mã độc, virus để phát hiện và ngăn chặn, loại bỏ mã độc.

Khi triển khai các nội dung nêu trên, trong trường hợp cần thiết, Quý đơn vị có thể liên hệ với Cục An toàn thông tin, số điện thoại: 024.3943.6684, thư điện tử ais@mic.gov.vn để được phối hợp, hỗ trợ.

Trân trọng./.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

Nguyễn Huy Dũng

Nơi nhận:
- Như trên;
- Lãnh đạo Bộ (để b/c);
- Cục trưởng (để b/c);
- Lưu: VT, TĐQLGS.