

Lây nhiễm mã độc đang diễn biến phức tạp tại Việt Nam

20:21 07/05/2019

Tình hình lây nhiễm phần mềm độc hại tại Việt Nam đang có diễn biến phức tạp, tiềm ẩn nhiều nguy cơ tấn công mạng nguy hiểm. Mã độc ở Việt Nam hiện có rất nhiều loại song 5 loại mã độc đang lây nhiễm nhiều nhất là: Virus USB, virus đào tiền ảo, virus mã hóa dữ liệu, phần mềm gián điệp và mã độc tấn công APT. Theo thống kê từ Trung tâm Giám sát an toàn không gian mạng quốc gia trực thuộc Cục An toàn thông tin, Bộ TT&TT, có khoảng 4,7 triệu địa chỉ IP



Theo thống kê từ hệ thống giám sát virus của Bkav, chỉ tính riêng trong năm 2018, loại virus có tên XFile USB đã lây nhiễm hơn 1,2 triệu máy tính ở Việt Nam. Và con số này chưa dừng lại ở đó khi chỉ trong tháng trước tại Việt Nam

đã có khoảng 3.900 trường hợp máy tính bị nhiễm virus mã độc mã hóa tổng tiền mới GandCrab thuộc thế hệ thứ 5 sau các virus nguy hiểm như Pettya, hay Wanna Cry.

Theo Ông Vũ Ngọc Sơn – PCT phụ trách mảng mã độc, Tập đoàn BKAV cho biết hiện nay đang xuất hiện một số mã độc mà chúng ta có thể nhận biết được đó là :

0804 Như chúng ta đã biết thế hệ mới nhất Grand Crab vừa xuất hiện ở VN đã là thế hệ thứ 5 rồi và thế hệ đầu tiên chỉ xuất hiện vào tháng 1-2018. Tức là 1 năm thôi mã độc này đã ra tới 5 biến thể.

1423 Mã độc mã hóa dữ liệu tổng tiền thì hiện nay nó đã xuất hiện ở những con đường khác nhau để có thể lây nhiễm vào máy tính người sử dụng, nó đã có thể lây nhiễm qua USB, tức là khi cắm USB từ máy tính bị nhiễm Virus sang máy tính không bị nhiễm thì Virus nó sẽ xâm nhập sang, nó cũng có thể lây qua email, như chúng ta đã biết con Grand Crab này đã lây qua email hoặc cũng có thể lây qua lỗ hổng phần mềm như Wanna Cry.

0037 Qua tình hình diễn biến phức tạp của mã độc nhất là trong thời gian gần đây thì nhất là các mã độc mà hướng tới mục đích kiếm lợi về tài chính, ví dụ như loại mã độc mã hóa tổng tiền hoặc mã độc đào tiền ảo thì bùng phát ở các cơ quan tổ chức. Và qua rà soát đánh giá thì hầu hết tại các hệ thống mạng của cơ quan tổ chức thì chúng tôi cũng đều phát hiện và ghi nhận thấy các loại mã độc với mục đích này đặc biệt là các loại mã độc đào tiền ảo và mã hóa tổng tiền. Có thể nói là tất cả các con đường mà máy tính có thể giao tiếp được với nhau thì mã độc mã hóa tổng tiền đều đã xuất hiện. Do đó người dùng cần phải trang bị các phương thức phòng ngừa mới cho các máy tính.

0155 Đối với 2019 thì chúng ta sẽ phải đối diện với rất nhiều nguy cơ trong đó những nguy cơ về tấn công vào các thiết bị như IOT, thiết bị Internet of things cũng như 1 số tấn công mới đòi hỏi chúng ta vẫn phải đối diện và chính vì thế chúng ta buộc phải sử dụng những công nghệ mới để phát hiện ra những nguy cơ này.

Để phòng chống virus, các chuyên gia an ninh mạng khuyến cáo, người dùng cần trang bị những kiến thức cần thiết và cài đặt phần mềm diệt virus thường trực cho máy tính được tự động cập nhật và bảo vệ tự động. Tuyệt đối không mở file đính kèm từ các email không rõ nguồn gốc. Có như vậy mới giảm thiểu được những rủi ro không đáng có trên môi trường không gian mạng.

Tâm An