

Cung cấp miễn phí 2 công cụ giúp nhận diện mã độc mã hóa dữ liệu tống tiền

06:42 08/09/2020

Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, Bộ TT&TT vừa cung cấp miễn phí cho cộng đồng 2 công cụ “Make in Vietnam” giúp nhận diện mã độc mã hóa dữ liệu tống tiền.

Nghiên cứu mới đây của Kaspersky chỉ ra rằng, tuy có giảm nhưng số lượng cuộc tấn công bằng mã độc mã hóa dữ liệu tống tiền (ransomware) vào Việt Nam vẫn ở mức cao.

Việt Nam xếp thứ 8 trên thế giới về số lượng máy tính bị tấn công bằng ransomware. Các chuyên gia an ninh mạng cũng liên tục cảnh báo về sự xuất hiện của nhiều loại ransomware mới.

Chuyên gia NCSC cho biết, là một dạng phần mềm độc hại, ransomware ngăn chặn người dùng có thể truy cập và sử dụng dữ liệu bên trong máy chủ (hoặc máy tính nói chung).



Ảnh minh họa (Ảnh: internet)

Kẻ tấn công sẽ yêu cầu một khoản tiền chuộc từ nạn nhân để khôi phục quyền truy cập dữ liệu. Tuy nhiên, ngay cả khi đã thanh toán theo yêu cầu của kẻ tấn công thì không phải lúc nào người dùng cũng lấy lại được dữ liệu.

Để hỗ trợ người dùng, NCSC cho ra mắt hai công cụ "Giải mã, nhận diện mã độc mã hóa tổng tiền" và "Tự động phân tích tập tin độc hại" được các chuyên gia của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) thuộc Cục An toàn thông tin, Bộ TT&TT phát triển và cung cấp miễn phí tại website <http://khonggianmang.vn> nhằm hỗ trợ các cá nhân, tổ chức, doanh nghiệp đảm bảo an toàn trên môi trường mạng.

Người dùng có thể tìm kiếm công cụ giải mã cho ransomware qua đuôi file hoặc tải file bị mã hóa lên để nhận diện. Sau đó, người dùng được khuyến nghị nên đọc kỹ hướng dẫn sử dụng trước khi tải và chạy công cụ. Trong trường hợp ransomware chưa có công cụ giải mã, cần liên hệ để nhận được thông báo của NCSC khi công cụ giải mã đó có sẵn.

Công cụ "Kiểm tra tập tin độc hại" mới được NCSC cung cấp trên trang Khonggianmang.vn, cho phép người dùng kiểm tra mức độ an toàn của những tập tin đáng ngờ nhận được từ email, mạng xã hội hay từ các thiết bị ngoại vi như USB.

Công cụ hướng tới việc hỗ trợ phân tích các file tin học văn phòng hay bị lợi dụng tấn công như các file có đuôi .docx, .xlsx, .pdf, .rar, .zip...(hỗ trợ file tập tin tối đa 10Mb).

Các chuyên gia của NCSC hướng dẫn người dùng tải những file nghi ngờ, không rõ nguồn gốc hoặc tìm kiếm trong cơ sở dữ liệu của NCSC mã băm của file đó.

Sau đó hệ thống sẽ phân tích và trả về kết quả kiểm tra, xác nhận file đó có nhiễm mã độc hay không? Các tệp tin được tải lên để kiểm tra đều được mã hóa sau khi phân tích và được xóa sau khoảng thời gian nhất định, cam kết bảo mật và riêng tư.

Trước đó, vào trung tuần tháng 4/2020, NCSC đã cho ra mắt website Khonggianmang.vn. Trang web này cung cấp loạt giải pháp kỹ thuật để hỗ trợ cơ quan, tổ chức đảm bảo an toàn thông tin tin khi làm việc từ xa.

PV