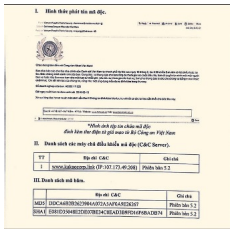

Trung tâm □ng c□u kh□n c□p máy tính Vi□t Nam phát thông báo kh□n yêu c□u các c□ quan, t□ ch□c tài chính, doanh nghi□p... kh□n c□p theo dõi, ngăn ch□n k□t n□i máy ch□ đi□u khi□n mã đ□c GandCrab 5.2 qua email gi□ m□o B□ Công an.

Trung tâm □ng c□u kh□n c□p máy tính Vi□t Nam (Trung tâm VNCERT) v□a có công văn kh□n g□i đ□n các c□ quan, t□ ch□c tài chính, doanh nghi□p… trong c□ n□□c thông báo v□ vi□c VNCERT v□a phát hi□n chi□n d□ch phát tán mã đ□c GandCrab 5.2 vào Vi□t Nam qua email gi□ m□o B□ Công an.

Theo VNCERT, GandCrab 5.2 là phiên b□n m□i trong h□ mã đ□c t□ng ti□n GandCrab lan r□ng trên toàn c□u trong h□n m□t năm qua.

Qua theo dõi không gian m□ng, Trung tâm VNCERT phát hi□n t□ gi□a tháng 3/2019 đ□n nay đang có chi□n d□ch phát tán mã đ□c t□ng ti□n GandCrab 5.2 vào Vi□t Nam và các n□□c Đông Nam Á.

T□i Vi□t Nam, GandCrab 5.2 đ□□c phát tán thông qua th□ đi□n t□ gi□ m□o B□ Công an Vi□t Nam v□i tiêu đ□ "Goi trong Cong an Nhan dan Viet Nam", có đính kèm t□p documents.rar.

Khi ng□□i dùng gi□i nén và m□ t□p tin đính kèm, mã đ□c s□ đ□□c kích ho□t và toàn b□ d□ li□u

người dùng bị mã hóa, đồng thời sinh ra một tập nhắm yêu cầu và hướng dẫn người dùng trả tiền chuộc từ 400 - 1.000 USD bằng cách thanh toán qua đồng tiền điện tử để giải mã dữ liệu.

Mã độc tống tiền GandCrab rất nguy hiểm, có thể đánh cắp thông tin và mã hóa toàn bộ dữ liệu trên máy bị nhiễm. Tin tức khai thác và tấn công sẽ gây nhiều hậu quả nghiêm trọng khác - ông Nguyễn Khắc Lịch, phó giám đốc Trung tâm VNCERT, nhận mạnh.

Trung tâm VNCERT yêu cầu lãnh đạo các đơn vị chỉ đạo các đơn vị thuộc phạm vi quản lý thực hiện khẩn cấp các việc sau để phòng ngừa, ngăn chặn việc tấn công của mã độc GandCrab 5.2 vào Việt Nam theo dõi, ngăn chặn kết nối đến các máy chủ máy chỉ điều khiển mã độc tống tiền GandCrab và cập nhật vào các hệ thống bảo vệ như: IDS/IPS, Firewall… theo các thông tin nhận dạng - công văn của VNCERT nêu rõ.

Nếu phát hiện cần nhanh chóng cô lập vùng/máy đã phát hiện.

Đồng thời, cần thông báo người sử dụng nâng cao cảnh giác, không mở và click vào các liên kết cũng như các tập tin đính kèm trong email có chứa các tập tin dạng .doc, .pdf, .zip, rar,… được gửi từ người lạ hoặc nếu email được gửi từ người quen nhưng cách đặt tiêu đề hoặc ngôn ngữ khác thường.

Và cần thông báo cho bộ phận chuyên trách quản trị hệ thống hoặc đảm bảo an toàn thông tin khi gặp nghi ngờ.

(TTO)