BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM
CÔNG NGHỆ THÔNG TIN

Số: 92 /CV-TTCNTT
V/v theo dõi, phòng ngừa, ngăn chặn mã độc GhostTeam và mã độc tống tiền GandCrab

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

Hà Nội, ngày 17 tháng 04 năm 2018

Kính gửi: Các đơn vị trực thuộc Bộ

Trong thời gian gần đây, các cơ quan chức năng đã phát hiện các chiến dịch phát tán mã độc GhostTeam và mã độc tống tiền GandCrab đang tấn công nhiều nước trên thế giới, trong đó có Việt Nam. Theo đó, mã độc GhostTeam được phát tán thông qua chợ ứng dụng Google Play, với thủ đoạn giả mạo các ứng dụng thường dùng như: quét mã vạch, ghi âm, trò chơi cờ vua,... Để vượt qua kiểm tra bảo mật của Google, GhostTeam không chứa mã độc khi tải lên Google Play, chỉ có tính năng hiển thị các quảng cáo. Tuy nhiên, khi chạy, ứng dụng này có thể tải các đoạn mã hoặc ứng dụng khác về thiết bị. GhostTeam thu thập thông tin về thiết bị (như: ID, vị trí, ngôn ngữ và thông số hiển thị), đánh cắp thông tin đăng nhập Facebook bằng cách lừa đảo người dùng đăng nhập các dịch vụ Google Play hoặc các ứng dụng giả mạo. Các mã JavaScript trong ứng dụng độc hại thường được phát tán qua nút "share" (chia sẻ) trên trang Facebook và lây nhiễm với "bạn bè" của nạn nhân. Với lượng lớn người dùng, hệ điều hành Android là hệ điều hành bị nhiều tin tặc nhắm tới, nên Android là hệ điều hành có nguy cơ bị lây nhiễm mã độc hàng đầu hiện nay. Mã độc tống tiền GandCrab được phát tán thông qua bộ công cụ khai thác lỗ hổng RIG, khi bị lây nhiễm, toàn bộ các tập tin dữ liệu trên máy tính người dùng sẽ bị mã hóa và phần mở rộng của tập tin bị đổi thành *.GDCB hoặc *CRAB, đồng thời mã độc sinh ra một tệp CRAB-DECRYPT.txt nhằm yêu cầu và hướng dẫn người dùng trả tiền chuộc từ 400 – 1000 USD bằng cách thanh toán qua tiền điện tử DASH để giải mã dữ liệu.

Do tính chất nguy hiểm của 02 mã độc nêu trên như có thể đánh cắp thông tin và mã hóa toàn bộ dữ liệu trên máy bị nhiễm. Tin tặc khai thác và tấn công sẽ gây ra nhiều hậu quả nghiêm trọng khác, Trung tâm Công nghệ thông tin đề nghị Quý Đơn vị/Cá nhân thực hiện nghiêm túc các công việc sau để phòng ngừa, ngăn chặn sự tấn công của mã độc GandCrab và GhostTeam:

1. Theo dõi, ngăn chặn kết nối đến các máy chủ máy chủ điều khiển mã độc tống tiền GandCrab và cập nhật vào các hệ thống bảo vệ như: IDS/IPS Firewall, ... các thông tin nhận dạng tại Phụ lục đính kèm;

2. Nếu phát hiện mã độc GandCrab cần nhanh chóng cô lập vùng/máy bị

nhiễm và báo cáo về Trung tâm Công nghệ thông tin;

3. Các cán bộ cần nâng cao cảnh giác, không mở và click vào các liên kết (link) cũng như các tập tin đính kèm trong email có chứa các tập tin dạng .doc, .pdf, .zip,... 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 nhận được email nghi ngờ;

4. Các cán bộ không cài đặt, sử dụng các phần mềm không rõ nguồn gốc trên điện thoại di động; cập nhật bản nâng cấp mới nhất của hệ điều hành;

5. Tăng cường công tác bảo vệ bí mật nhà nước, tuyên truyền, phổ biến kiến thức bảo mật cho cán bộ.

Mọi chi tiết xin liên hệ Trung tâm Công nghệ thông tin: Địa chỉ: Phòng 503, 113 Trần Duy Hưng, Cầu Giấy, Hà Nội; Điện thoại: 024 39439060.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Phạm Đại Dương (để b/c);
- Lưu: TTCNTT.

GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

PHỤ LỤC

THÔNG TIN VỀ MÃ ĐỘC GANDCRAB

I. Danh sách các máy chủ điều khiển mã độc GandCrab (C&C Server) cập nhật đến ngày 05/4/2018

TT	Địa chỉ C&C
1	politiaromana.bit
2	malwarehunterteam.bit
3	gdcb.bit

II. Danh sách mã băm (Hash SHA-256)

TT	SHA-256
1	966a0852c8adbea0b7b7aada7c2c851ee642c7bca7da3b29eel43f47ddeb90a5