UBND TỈNH SƠN LA
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc Lập – Tự Do – Hạnh Phúc

Số: 984 /STTTT-CNTT
V/v cảnh báo mã độc Trickbot có thể đánh sập ứng dụng bảo mật Windows Defender trên Windows 10

Sơn La, ngày 02 tháng 8 năm 2019

Kính gửi:
- Văn phòng tỉnh ủy, HĐND, UBND tỉnh;
- Các Sở, ban, ngành;
- Công an tỉnh Sơn La;
- Ban Chỉ huy quân sự tỉnh Sơn La;
- UBND các huyện, thành phố;
- Trung tâm CNTT&TT;
- Các Hội, Đoàn thể của tỉnh;

Trojan Trickbot là một mã độc ngân hàng nhắm tới khách hàng của một số ngân hàng lớn với chiến dịch spam email mới nhằm hướng nạn nhân tới một trang đăng nhập giả mạo mà không thể phân biệt được với website chính thức của ngân hàng.

Hiện tại, loại **mã độc** ngân hàng này không còn chỉ "né tránh" mà có khả năng đánh sập ứng dụng bảo mật Windows Defender trên hệ điều hành Windows 10 của người dùng. Tin tặc lợi dụng công cụ này để đánh cắp thông tin tài khoản ngân hàng online và ví tiền điện tử. Theo cảnh báo của các chuyên gia an ninh mạng, Hệ điều hành của Microsoft luôn là môi trường bị tin tặc sử dụng để phát tán mã độc Trickbot thông qua hình thức "ngụy trang" các văn bản như Word và Excel. Do đó, có tới 250 triệu người dùng Windows 10 bị đe dọa bởi mã độc Trickbot, trong đó có Việt Nam.

Chiến dịch mới nhất hiện nay đang nhắm tới những người dùng Windows 10 bằng một thông báo trên trang miền Office 365 được thiết kế tinh vi và chi tiết để nhắc nhở cập nhật qua đó cài đặt loại Trojan này lên thiết bị cá nhân. Khi xâm nhập vào máy tính, Trickbot sẽ tìm cách vô hiệu hóa, xóa dịch vụ và chấm dứt các tiến trình liên quan đến Windows Defender. Ngoài ra, nó cũng thâm nhập vào mục Windows Group Policy để vô hiệu hóa hoàn toàn Windows Defender đồng thời tắt các thông báo bảo mật.

Hiện vẫn chưa có "phương thuốc" cụ thể để phát hiện và bảo vệ máy tính an toàn từ nguy hiểm trên.

Nhằm bảo đảm an toàn thông tin, phòng tránh nguy cơ trở thành mục tiêu của chiến dịch này Sở Thông tin và Truyền thông khuyến nghị Thủ trưởng các cơ quan, đơn vị nghiêm túc quán triệt, chỉ đạo các cán bộ, công chức, viên chức:

1. Không tắt ứng dụng Windows Defender; thường xuyên kiểm tra cập nhật Windows từ Microsoft và tải bản cập nhật mới nhất trên Windows 10 để bảo vệ dữ liệu.

2. Hạn chế tải và đọc những tài liệu không rõ nguồn gốc, qua các tên miền lạ hay tin nhắn messenger không rõ địa chỉ.

3. Hãy ghi mật khẩu ngân hàng, tín dụng trên điện thoại, sổ tay như là phương án thay thế lưu mật khẩu tự động trên trình duyệt của máy tính.

4. Theo dõi, giám sát hệ thống để phát hiện sớm, kịp thời phản ứng các hành vi dò quét/tấn công mạng.

Trân trọng đề nghị các cơ quan, đơn vị quan tâm, thực hiện./.

Nơi nhận:
- Như trên;
- Thường trực UBND tỉnh (để báo cáo);
- Ban Giám đốc;
- Lưu VT, CNTT (Tr 39b).

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Ký bởi: Phạm Quốc Chinh
Email: chinhpq.stttt@sonla.gov.vn
Cơ quan: Sở Thông tin và Truyền thông, Tỉnh Sơn La
Ngày ký: 02.08.2019 16:35:31 +07:00

Phạm Quốc Chinh