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: 945 /STTTT-CNTT
V/v cảnh báo virus W32.CrashSMB gây khởi động lại máy tính đột ngột đang bùng phát tại Việt Nam

Sơn La, ngày 27 tháng 8 năm 2018

Kính gửi:
- Văn phòng tỉnh ủy;
- Văn phòng Hội đồng nhân dân tỉnh;
- Văn phòng Ủy ban nhân dân tỉnh;
- Các Sở, ban, ngành;
- UBND các huyện, thành phố.
- Công an tỉnh; Ban Chỉ huy Quân sự tỉnh;
- Trung tâm Hành chính công;
- Trung tâm Công nghệ thông tin và Truyền thông.

Theo cảnh báo của các chuyên gia an ninh mạng, hàng loạt hệ thống mạng tại Việt Nam với số lượng máy tính lớn đã bị đình trệ bởi loại virus mới nguy hiểm có tên **W32.CrashSMB** gây ra hiện tượng máy tính đang sử dụng bị lỗi khởi động lại đột ngột hoặc bị lỗi màn hình xanh (Blue Screen). Tính đến nay đã có 329.000 máy tính tại Việt Nam được ghi nhận nhiễm loại virus nguy hiểm W32.CrashSMB, trong đó **tỉnh Sơn La** có khoảng 10 máy tính đã bị lây nhiễm, đã được Sở Thông tin và Truyền thông hướng dẫn xử lý kịp thời.

Phân tích của các chuyên gia cho hay, loại virus W32.CrashSMB được phát tán bằng kỹ thuật tấn công, khai thác các máy tính tồn tại lỗ hổng SMB. Đây là hình thức tấn công tương tự như của virus mã hóa dữ liệu tống tiền "nổi tiếng" WannaCry đã sử dụng. Lỗ hổng phần mềm SMB - lỗ hổng virus WannaCry từng sử dụng đã nhiều lần được các chuyên gia an toàn thông tin mạng cảnh bảo về mức độ nguy hiểm của nó. Theo ước tính, vẫn có tới hơn 50% máy tính tại Việt Nam chưa được vá lỗ hổng SMB và thậm chí ngay cả với một số máy tính mới được người dùng mua về từ cửa hàng cũng tồn tại lỗ hổng bảo mật nguy hiểm này.

Cũng theo phân tích, sau khi lây nhiễm, virus W32.CrashSMB sẽ chiếm quyền điều khiển máy tính, biến máy của nạn nhân thành một máy tính ma, từ đó tiếp tục tấn công sang các máy khác trong cùng hệ thống mạng. "*Dấu hiệu dễ thấy khi một máy tính bị virus W32.CrashSMB tấn công là thỉnh thoảng hệ điều hành hiện thông báo lỗi, sau đó máy tính bị khởi động lại đột ngột hoặc bị lỗi màn hình xanh (Blue Screen)*".

Khi bị virus W32.CrashSMB chiếm quyền điều khiển máy tính, người dùng sẽ phải đối mặt với các nguy cơ bị theo dõi, bị lấy cắp dữ liệu và thông tin cá nhân, lấy cắp tài khoản ngân hàng, tài khoản Gmail, Facebook… Đồng thời, máy tính của người dùng cũng sẽ bị chạy rất chậm vì virus W32.CrashSMB sử dụng tài nguyên hệ thống để thực hiện hành vi đào tiền ảo.

Nhằm đảm bảo an toàn thông tin mạng, phòng/chống nguy cơ lây nhiễm virus W32.CrashSMB, Sở Thông tin và Truyền thông cảnh báo và đề nghị các cơ quan, đơn vị nghiêm túc triển khai một số nội dung:

1. Thường xuyên cập nhật bản vá mới nhất của hệ điều hành.

2. Cài đặt phần mềm diệt virus thường trực để được bảo vệ một cách tự động; cập nhật phiên bản mới nhất của phần mềm diệt virus để cập nhật mẫu nhận diện virus W32.CrashSMB.

3. Nghiêm túc triển khai thực hiện các hướng dẫn của Sở Thông tin và Truyền thông, tại công văn số 920/STTTT-CNTT ngày 21/8/2018 về việc tăng cường bảo đảm an toàn thông tin trong dịp Lễ Quốc khánh 02/9 và công tác đảm bảo an toàn thông tin trên môi trường mạng.

4. Cán bộ chuyên trách/kiêm nhiệm công nghệ thông tin, quản trị mạng tại các cơ quan, đơn vị thường xuyên theo dõi, rà soát hệ thống máy tính của cơ quan, đơn vị mình; kịp thời báo cáo, phối hợp xử lý các sự cố xảy ra.

Thông tin hỗ trợ vui lòng liên hệ: Phòng Công nghệ thông tin, Sở Thông tin và Truyền thông tỉnh Sơn La; số 20 đường Hoàng Quốc Việt, TP Sơn La, Tỉnh Sơn La, Điện thoại: 0212 2210.468;

Đề nghị các cơ quan, đơn vị quan tâm, thực hiện./.

Nơi nhận:
- Như trên;
- Thường trực UBND tỉnh;
- Bộ Thông tin và Truyền thông;
- Cục An toàn thông tin;
- Trung tâm VNCERT;
- Lưu VT, CNTT (Tr 40b).

Để báo cáo

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Ký bởi: Phạm Quốc Chinh
Email: chinhpq.sttt@sonla.gov.vn
Cơ quan: Sở Thông tin và Truyền thông, Tỉnh Sơn La
Ngày ký: 27.08.2018 09:49:00 +07:00

Phạm Quốc Chinh