UBND TỈNH SƠN LA
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 1662 /STTTT-CNTTVT

Sơn La, ngày11tháng 11 năm 2024

V/v tăng cường rà soát về chiến dịch tấn công có chủ đích vào mạng công nghệ thông tin các cơ quan Đảng và nhà nước

Kính gửi:
- Văn phòng tỉnh ủy, HĐND, UBND tỉnh;
- Các Sở, ban, ngành;
- Mặt trận tổ quốc và các Đoàn thể của tỉnh;
- UBND các huyện, thành phố;
- Trung tâm Công nghệ thông tin và Truyền thông;
- Viễn thông Sơn La, Viettel Sơn La.

Theo thông tin từ Ban Cơ yếu Chính phủ, một chiến dịch tấn công có chủ đích đang nhằm vào các hệ thống công nghệ thông tin (CNTT) của các cơ quan Đảng và Nhà nước, đặc biệt là các cơ quan Trung ương. Chiến dịch này có mục tiêu thu thập và đánh cắp thông tin, dữ liệu quan trọng với các đặc điểm chính như sau:

- Chiến dịch tập trung tấn công vào mạng công nghệ thông tin (CNTT) của các cơ quan Đảng và Nhà nước tại Trung ương, nơi lưu trữ nhiều thông tin dữ liệu mật và tài liệu quan trọng.

- Mã độc được thiết kế đặc thù cho từng hệ thống CNTT, gây khó khăn cho các chương trình phòng chống mã độc hiện có trong việc phát hiện. Mã độc lây nhiễm vào máy tính người dùng (hệ điều hành Windows) để đánh cắp dữ liệu, dữ liệu sau đó được mã hóa, lưu trữ ẩn trong máy tính bị nhiễm và chuyển đến máy chủ của tin tặc.

- Mã độc này còn có khả năng lây nhiễm sang các thiết bị USB chuyên dụng, được sử dụng để sao chép dữ liệu mật và quan trọng, mã độc còn có thể lây nhiễm thu thập dữ liệu ngay cả trong mạng nội bộ.

(Gửi kèm Danh sách và dấu hiệu nhận biết một số dòng mã độc)

- Thời gian triển khai chiến dịch tấn công không được xác định rõ ràng. Qua điều tra, một số mạng CNTT đã phát hiện mã độc tồn tại từ vài tháng đến vài năm, dẫn đến khó khăn trong việc đánh giá mức độ thất thoát dữ liệu.

Trước tình hình trên, Sở Thông tin và Truyền thông đề nghị:

1. Các sở, ban, ngành, UBND các huyện, thành phố

- Quán triệt tuyên truyền, nâng cao nhận thức cho cán bộ, công chức, viên chức về nguy cơ mất an toàn thông tin, đặc biệt đối với các thông tin thuộc danh mục bí mật nhà nước khi sử dụng mạng máy tính.

- Tiến hành rà soát, đánh giá tổng thể toàn bộ hệ thống CNTT nhằm kịp thời phát hiện và xử lý mã độc, đảm bảo bảo vệ dữ liệu của cơ quan, đơn vị.

- Thực hiện nghiêm quy định bảo vệ thông tin bí mật nhà nước:

+ Thông tin bí mật nhà nước truyền qua mạng viễn thông, internet và các thiết bị lưu trữ kết nối mạng phải được mã hóa bằng mật mã cơ yếu.

+ Thông tin bí mật nhà nước trên các thiết bị không kết nối mạng phải tuân thủ quy định tại khoản 2 và khoản 3 Điều 12 Luật Bảo vệ bí mật nhà nước và được mã hóa bằng mật mã cơ yếu khi có yêu cầu.

2. Trung tâm Công nghệ thông tin và Truyền thông

Chủ động rà soát lại toàn bộ Hệ thống thông tin tại Trung tâm tích hợp dữ liệu tỉnh đồng thời cập nhật các giải pháp bảo mật để phát hiện và xử lý kịp thời các dấu hiệu tấn công.

3. Đề nghị VNPT Sơn La, Viettel Sơn La

Chủ động rà soát các hệ thống dịch vụ, bảo đảm an toàn thông tin, đặc biệt tổ chức hệ thống dự phòng, sẵn sàng duy trì tính sẵn sàng cho các dịch vụ do đơn vị cung cấp.

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

Nơi nhận:
- Như trên;
- Công an tỉnh;
- Ban Giám đốc (b/c);
- Trang TTĐT Sở TT&TT;
- Lưu: VT, CNTTVT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH SƠN LA

Phạm Quốc Chinh

Phụ lục
DANH SÁCH VÀ DẤU HIỆU NHẬN BIẾT MỘT SỐ DÒNG MÃ ĐỘC THUỘC CHIẾN DỊCH TẤN CÔNG CÓ CHỦ ĐÍCH VÀO MẠNG CNTT CÁC CƠ QUAN ĐẢNG VÀ NHÀ NƯỚC

STT	LOẠI MÃ ĐỘC	MÃ HÀM BĂM	MÔ TẢ HÀNH VI
1	Backdoor.Win64.Rgsc.a	MD5: c4a8e185f8331e5d75d4eef592 a7320a	Mở cửa hậu kết nối để thực hiện những truy cập bất hợp pháp và đưa các mã độc khác vào hệ thống.
		SHA-1: 9c0e748941cde7fcf5ca70fd9c 41434f13df5c1	
		SHA-256: f4064d63551dcf913dd5fe008e a45a629271a389d7bde143346 c3e0 c9b32a130	
2	Trojan.Win32.Agentgen	MD5: c3eb16f61c0c9ecd66b69da3ef5d bd5f	Nằm vùng, đánh cắp dữ liệu, sau đó gửi dữ liệu tới máy chủ của tin tặc.
		SHA-1: 147f745a13c19affed8ad8f799cb c607cde3086e	
		SHA-256: 6252c96828cf4d0f8df35528898 bbd8dbec566442e458d17d363e6 155107414f	
3	Trojan.Win32.Zenpak.e usi	MD5: 224bf90c6c204bbcddf7a7e6440 9187c	Nằm vùng, đánh cắp dữ liệu, sau đó gửi dữ liệu tới máy chủ của tin tặc, kết nối ra ngoài tới địa chỉ 10.229.166.255
		SHA-1: 6dc3860db0c1dda0f3d09bcf0aa6 9e025980406d	
		SHA-256: 6557233314c95c1de72f8d10cb7 5c69be65711ddda7e2b78dbdddf a475bc2499	
4	UDS.Trojan Win64.Agent.a	MD5: 7c2a917105078b004c988f71a41 9f481	Nằm vùng, đánh cắp dữ liệu, sau đó gửi dữ liệu tới máy chủ của tin tặc
		SHA-1: bce588cf49038af06f0848cbe 072b5f5lele581c	
		SHA-256: 3b0ad11d32ce6f71f44abce08239	

		dab57a2c3029db46ef3d8945ff91 eea35b8e	