UBND TỈNH ĐỒNG NAI
SỞ Y TẾ

Số: 3234 /SYT-VP

V/v triển khai Thông báo số 19/TB-BCA-A05 ngày 12/5/2020 của Bộ Công an

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

Đồng Nai, ngày 16 tháng 6 năm 2020

Kính gửi: Giám đốc, Thủ trưởng các đơn vị trực thuộc.

Thực hiện Công văn số 5859/UBND-KGVX ngày 25/5/2020 của UBND tỉnh về việc thực hiện Thông báo số 19/TB-BCA-A05 ngày 12/5/2020 của Bộ Công an về chiến dịch tấn công của các nhóm tội phạm mạng nhằm vào các trang, cổng thông tin điện tử của cơ quan nhà nước (*Đính kèm Thông báo*).

Giám đốc Sở Y tế đề nghị Giám đốc, Thủ trưởng các đơn vị trực thuộc chỉ đạo các tổ chức, cá nhân phụ trách về công nghệ thông tin của đơn vị nghiêm túc triển khai thực hiện nội dung Thông báo số 19/TB-BCA-A05 ngày 12/5/2020 của Bộ Công an.

Đề nghị Giám đốc, Thủ trưởng các đơn vị trực thuộc triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Lưu: VT, VP.

GIÁM ĐỐC

Phan Huy Anh Vũ

Số 2 - Phan Đình Phùng, phường Quang Vinh, thành phố Biên Hoà, tỉnh Đồng Nai
ĐT: (02513) 942641, Fax: (02513) 847269, Email: syt@dongnai.gov.vn, Website: syt.dongnai.gov.vn

BỘ CÔNG AN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 19/TB-BCA-A05	*Hà Nội, ngày 12 tháng 5 năm 2020*

THÔNG BÁO

Về chiến dịch tấn công của các nhóm tội phạm mạng nhằm vào các trang, cổng thông tin điện tử của cơ quan nhà nước

Thời gian gần đây, qua công tác nắm tình hình trên không gian mạng, Bộ Công an phát hiện chiến dịch tấn công của các nhóm tội phạm mạng nhằm vào các trang, cổng thông tin điện tử (TTĐT) thuộc quản lý của cơ quan nhà nước với phương thức, thủ đoạn như sau:

1. Hoạt động tấn công, xâm nhập, kiểm soát hệ thống mạng

1.1. Thu thập toàn bộ thông tin, dữ liệu công khai trên mạng Internet về hệ thống trang, cổng TTĐT của cơ quan nhà nước. Đặc biệt là các hệ thống trang, cổng TTĐT sử dụng các giải pháp công nghệ của Microsoft như công nghệ ASP.NET, SharePoint.

1.2. Tiến hành rà quét, khai thác lỗ hổng bảo mật tồn tại trên các trang, cổng TTĐT, đặc biệt là các lỗ hổng cho phép tin tặc kích hoạt thực thi mã độc từ xa để kiểm soát hệ thống máy chủ web, như: CVE-2017-11317 và CVE-2019-18935 tồn tại trên thư viện "Telerik UI" của các website sử dụng ngôn ngữ lập trình ASP.NET. Qua kiểm tra rà soát, cơ quan chức năng của Bộ Công an phát hiện **704** trang, cổng TTĐT của cơ quan nhà nước có sử dụng thư viện "Telerik UI", trong đó có **28** trang, cổng TTĐT tồn tại lỗ hổng bảo mật có thể bị tin tặc tấn công, khai thác từ xa.

1.3. Khi đã kiểm soát thành công máy chủ web, các nhóm tin tặc tiếp tục sử dụng các công cụ tấn công chuyên dụng, rà quét toàn bộ hệ thống mạng, khai thác lỗ hổng bảo mật MS17-010 trên hệ điều hành Windows để tấn công lây lan, chiếm quyền kiểm soát các máy tính trong hệ thống mạng, lợi dụng các điểm yếu trong thiết kế và cấu hình hệ thống để tấn công leo thang đặc quyền, xâm nhập vào hệ thống mạng nội bộ, từ đó có thể kiểm soát toàn bộ hệ thống thông tin của các cơ quan nhà nước, chiếm đoạt thông tin, tài liệu nội bộ, tài liệu chứa BMNN.

2. Hoạt động tấn công, chèn nội dung quảng cáo game bài đổi thưởng

Lợi dụng lỗ hổng bảo mật của thư viện "Telerik UI" và việc không kiểm duyệt chặt chẽ nội dung đăng tải, một số nhóm tội phạm mạng đã tấn công, xâm nhập vào các trang, cổng TTĐT của cơ quan nhà nước để chèn, đăng tải trái phép đường dẫn, hình ảnh quảng cáo cho game bài nhằm gia tăng tính tin cậy trên kết quả tìm kiếm bằng công cụ Google search, thu hút người chơi tham gia; ảnh hưởng nghiêm trọng đến uy tín của cơ quan nhà nước và trật tự an toàn xã hội. Qua rà soát, Bộ Công an phát hiện **14** trang, cổng TTĐT của cơ quan nhà nước tồn tại đường dẫn, hình ảnh quảng cáo cho game bài V8 Club.

Từ tình hình trên, để bảo đảm an ninh mạng, Bộ Công an đã chỉ đạo đơn vị chức năng phối hợp với các đơn vị chủ quản trang, cổng TTĐT tồn tại lỗ hổng bảo mật điều tra, xác minh, xử lý theo quy định của pháp luật; đồng thời đề nghị các bộ, ban, ngành, địa phương chủ động thực hiện các biện pháp sau:

- Tổ chức kiểm tra, rà soát, khắc phục lỗ hổng bảo mật trên các trang, cổng TTĐT, đặc biệt là lỗ hổng tồn tại trên thư viện "Telerik UI"; gỡ bỏ các đường dẫn, hình ảnh quảng cáo game bài (nếu có);

- Tăng cường giám sát an ninh mạng, kịp thời phát hiện hoạt động tấn công mạng, phối hợp với đơn vị chức năng của Bộ Công an trong điều tra, xác minh, xử lý đối tượng thực hiện tấn công mạng.

Bộ Công an xin thông báo./.

Nơi nhận:
- Đ/c Bộ trưởng Tô Lâm (để báo cáo);
- Các đồng chí Thứ trưởng (để báo cáo);
- Văn phòng TW Đảng
- Văn phòng Tổng Bí thư
- Văn phòng Chủ tịch nước
- Văn phòng Quốc hội
- Văn phòng Chính phủ
- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ (để phối hợp);
- Tỉnh ủy, Thành ủy, UBND các tỉnh, TP trực thuộc TW
- Tòa án nhân dân tối cao
- Viện kiểm sát nhân dân tối cao
- Kiểm toán nhà nước
- Các tập đoàn, tổng công ty: EVN, PVN, VNA, VATM, ACV (để phối hợp);
- Công an các đơn vị trực thuộc Bộ
- Công an các tỉnh, thành phố trực thuộc TW (để thực hiện);
- Lưu: VT, A05(P8).

TUQ. BỘ TRƯỞNG
CỤC TRƯỞNG CỤC AN NINH MẠNG VÀ PCTP SỬ DỤNG CÔNG NGHỆ CAO

Thiếu tướng Nguyễn Minh Chính

DANH SÁCH CÁC TRANG, CỔNG TTĐT TỒN TẠI LỖ HỔNG "TELERIK UI"

(Kèm theo Thông báo số 19/TB-BCA-A05 ngày 12/05/2020)

STT	Tên miền	Tên trang, cổng TTĐT
	xquang.dost-dongnai.gov.vn	Hệ Thống Quản Lý An Toàn Bức Xạ Và Hạt Nhân