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

Số: 139 /TTCNTT-KTHT
V/v Rà soát, gỡ bỏ mã độc trên trang, cổng thông tin điện tử

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

Hà Nội, ngày 20 tháng 05 năm 2020

Kính gửi: Các đơn vị trực thuộc Bộ có trang, cổng thông tin điện tử

Thực hiện Công văn số 19/TB-BCA-A05 ngày 12/05/2020 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. Sau khi nghiên cứu các tài liệu, Trung tâm Công nghệ thông tin thông báo và đề nghị các đơn vị trực thuộc Bộ có trang, cổng thông tin điện tử (TTĐT) thực hiện các biện pháp để bảo đảm an ninh mạng như sau:

1. Cách thức tấn công, xâm nhập, kiểm soát hệ thống mạng của tin tặc

- Tin tặc thực hiện 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.

- 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.

- 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 MS 17-010 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 của tin tặc

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.

3. Các biện pháp để bảo đảm an ninh mạng

- Thực hiện kiểm tra, rà soát mã nguồn trên các trang, cổng TTĐT để khắc phục lỗ hổng tồn tại trên thư viện "Telerik UI"; gỡ bỏ các đường dẫn, hình ảnh quảng cáo game (nếu có).

- Cập nhật các bản vá lỗ hổng trên hệ điều hành.

- Cập nhật phiên bản "Microsoft .NET framework" lên phiên bản mới nhất (Chú ý: không sử dụng các phiên Microsoft .NET framework từ 4.5 trở xuống).

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

Mọi thông tin xin liên hệ: Trung tâm Công nghệ thông tin, 113 Trần Duy Hưng, Cầu Giấy, Hà Nội; Số điện thoại: (024) 39439060; Hòm thư điện tử: phongktht@most.gov.vn

Trân trọng./.

Nơi nhận:
- Như trên;
- Lưu: VP, Phòng KTHT.

GIÁM ĐỐC

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

Ký bởi: Trung tâm Công nghệ thông tin
Cơ quan: Bộ Khoa học và Công nghệ
Ngày ký: 20.05.2020 14:29:04 +07:00

Hà Quốc Trung