

Kính gửi: Các đơn vị y tế trực thuộc

Thực hiện công văn số 336/CNTT-CSHT ngày 11/8/2017 của Cục công nghệ thông tin, Bộ Y tế về việc theo dõi, phòng chống mã độc Petya;

Theo cảnh báo của các đơn vị chuyên môn về An toàn thông tin, từ tối ngày 27/6/2017, có hàng nghìn cuộc tấn công mạng bằng biến thể của mã độc tổng tiền “Petya” trên thế giới, lây nhiễm trên 2000 mục tiêu là các mạng máy tính nội bộ của nhiều quốc gia, nhất là ở Nga, Ukraina, Ba Lan, Đức. Petya là một dạng mã độc tổng tiền (ransomware) rất nguy hiểm, khai thác lỗ hổng bảo mật “Eternal Blue” của giao thức SMBv1 (giao thức chia sẻ tệp tin của hệ điều hành Windows) tương tự như mã độc WannaCry, đồng thời kết hợp sử dụng kỹ thuật tấn công tinh vi khác để tán phát mã độc trong mạng nội bộ.

Nhằm phòng ngừa, ngăn chặn việc tấn công của mã độc Petya Sở Y tế đề nghị các đơn vị y tế trong toàn ngành thực hiện khẩn cấp các việc sau đây.

1. Đối với bộ phận chuyên trách Công nghệ thông tin tại các đơn vị

Tiếp tục triển khai các biện pháp phòng ngừa theo công văn số 676/SYT-VP ngày 22/5/2017 của Sở Y tế Hà Giang về việc theo dõi phòng chống mã độc WannaCry, khẩn trương cài đặt bản vá MS17-010 cho các máy tính và máy chủ của đơn vị mình. Để chủ động ngăn ngừa, ngăn chặn mã độc mã hóa dữ liệu, có thể tạo tệp Perfc tại đường dẫn “C:\Windows\perfc” và thiết lập thuộc tính chỉ đọc (read only), hoặc tải và thực thi tệp tin tại địa chỉ:

<https://download.bleepingcomputer.com/bats/nopetyavac.bat>.

2. Đối với các đơn vị quản lý mạng theo mô hình tập trung (domain), ngoài các biện pháp nêu trên cần triển khai các biện pháp kỹ thuật siết chặt chính sách bảo mật theo hướng dẫn của Microsoft tại địa chỉ:

<https://www.microsoft.com/en-us/download/details.aspx?id=36036> để ngăn chặn mã độc tấn công, kiểm soát toàn bộ hệ thống mạng. Trường hợp phát hiện mã độc Petya lây nhiễm vào hệ thống, đề nghị các đơn vị cô lập các máy tính bị lây nhiễm, thông báo về Cục công nghệ thông tin bộ Y tế hoặc Sở Y tế Hà Giang để phối hợp ngăn chặn xử lý.

Nhận được công văn này yêu cầu các đơn vị nghiêm túc triển khai thực hiện./.

**Nơi nhận:**

- Như trên;
- BGD, Các phòng thuộc sở;
- Trang thông tin điện tử ngành;
- VNPTiOffice;
- Lưu: VT, VP.

**GIÁM ĐỐC****Lương Viết Thuận**