BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 338/CATTT-TĐQLGS
V/v cảnh báo về biến thể mới của mã độc tống tiền Ransomware (mã độc Petya)

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

Hà Nội, ngày 28 tháng 6 năm 2017

Kính gửi:

- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn kinh tế; Tổng công ty nhà nước; Tổ chức tài chính và Ngân hàng.

Mã độc tống tiền, mã độc mã hóa dữ liệu (Ransomware) từ khi xuất hiện đã gây thiệt hại không nhỏ cho nhiều tổ chức, doanh nghiệp. Sau đợt tấn công hồi tháng 5 của mã độc tống tiền WannaCry, ngày 27/6/2017 mã độc Ransomware lại tiếp tục gây ảnh hưởng tới nhiều nước trên thế giới.

Biến thể mã độc lần này có tên Petya (còn gọi là Petwrap) không chỉ khai thác và lây lan thông qua lỗ hổng MS17-010 mà còn có thể lây nhiễm vào máy tính đã vá lỗ hổng này thông qua công cụ WMIC (công cụ có sẵn trong Windows cho phép truy cập và thiết lập cấu hình trên các máy Windows); công cụ PSEXE (công cụ cho phép truy cập vào máy tính Windows từ xa mà người dùng không biết thông qua dịch vụ SMB) và lỗ hổng CVE-2017-0199 (lỗ hổng trong Microsoft Office/WordPad cho phép tin tặc chiếm quyền điều khiển hệ thống).

Các lỗ hổng trên đã có bản vá, tuy nhiên có nhiều máy tính vẫn chưa cập nhật và có thể là nạn nhân của đợt tấn công lần này.

Petya có hoạt động rất khác so với các biến thể Ransomware khác. Petya khi lây nhiễm vào máy tính sẽ không mã hóa từng tập tin, mà thực hiện mã hóa Bảng File (Master File Table – MFT, chứa thông tin về tất cả các tập tin và thư mục trong phân vùng) và thay thế Master Boot Record của máy tính bằng tập tin độc hại để hiển thị thông tin đòi tiền chuộc. Do vậy máy tính người dùng sẽ không thể khởi động được khi bị nhiễm mã độc này.

Một số hòm thư điện tử dùng để phát tán mã độc Petya:

wowsmith123456@posteo.net

iva76y3pr@outlook.com

carmellar4hegp@outlook.com

amanda44i8sq@outlook.com

Khi lây nhiễm máy tính có kết nối mạng đến một số địa chỉ: 185.165.29.78; 84.200.16.242; 111.90.139.247; 95.141.115.108 (Nguồn: https://gist.githubusercontent.com/vulnersCom/65fe44d27d29d7a5de4c176baba45759/raw/b414f3162198d7fa117bb934a92124d7075b3f5e/Petya_ransomware.txt).

Cục An toàn thông tin đề nghị các cơ quan, tổ chức tăng cường các biện pháp bảo đảm an toàn thông tin để giảm thiểu nguy cơ từ mã độc Petya như sau:

- Kiểm tra và bảo đảm các máy tính trong hệ thống mạng đã vá các bản vá bảo mật, đặc biệt là MS17-010, CVE 2017-0199;

- Chặn toàn bộ kết nối liên quan đến dịch vụ SMB (445/137/138/139) từ ngoài Internet;

- Vô hiệu hóa WMIC (Windows Management Instrumentation Command-line);

- Không truy cập vào các liên kết lạ, cảnh giác cao khi mở các tập tin đính kèm trong thư điện tử;

- Sao lưu các dữ liệu quan trọng thường xuyên vào các thiết bị lưu trữ riêng biệt;

- Cập nhật phần mềm diệt virus;

- Tắt dịch vụ SMB trên tất cả các máy trong mạng LAN (nếu không cần thiết) ;

- Tạo tệp tin " C:\Windows\perfc " để ngăn ngừa nhiễm ransomware. Đây là tập tin mã độc kiểm tra trước thực hiện các hành vi độc hại trên máy tính.

Khi triển khai các nội dung nêu trên, trong trường hợp cần thiết, Quý đơn vị có thể liên hệ với Cục An toàn thông tin, số điện thoại: 04.3943.6684, thư điện tử ais@mic.gov.vn để được phối hợp, hỗ trợ.

Trân trọng./.

Nơi nhận:
- Như trên;
- Lãnh đạo Bộ (để b/c);
- Cục trưởng (để b/c);
- Cơ quan đơn vị thuộc Bộ;
- Lưu: VT, TĐQLGS.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HOÀ X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Huy Dũng