

Số: 126/CV-BKAV17

Hà Nội, ngày 30 tháng 05 năm 2017

V/v: Cảnh báo mã độc mới EternalRocks

SỞ THÔNG TIN VÀ TRUYỀN THÔNG

2131

Kính gửi: Sở Thông tin và Truyền thông Thành phố Cần Thơ

Bkav là đơn vị làm việc trong lĩnh vực về an ninh mạng tại Việt Nam.

Chuyên...

Mấy ngày qua xuất hiện mã độc mới EternalRocks khai thác các lỗ hổng dịch vụ SMB để phát tán trên các thiết bị Windows. Mã độc này không nhằm mục đích tống tiền như WannaCry (trong cảnh báo trước của Bkav) mà âm thầm nằm vùng, có thể được sử dụng để thực hiện các cuộc tấn công có chủ đích APT.

Sau khi lây nhiễm vào máy tính, để tránh bị phát hiện, EternalRocks tải về trình duyệt ẩn danh Tor, sau đó dùng trình duyệt này kết nối với máy chủ điều khiển (C&C server). Đồng thời, mã độc cũng "ẩn mình" 24 giờ sau mới kết nối tới máy chủ điều khiển và tải về các công cụ khai thác lỗ hổng SMB. Tiếp đến, EternalRocks quét trên mạng, tìm ra các máy tính có lỗ hổng SMB và tự lây nhiễm sang.

Với 52% máy tính tại Việt Nam, tức là khoảng 4 triệu máy chưa được vá các lỗ hổng SMB – các lỗ hổng đang bị WannaCry và EternalRocks khai thác để tấn công, nguy cơ mất an ninh là rất lớn.

Tham khảo thêm thông tin:

Mã độc mới EternalRocks có thể lây rộng hơn WannaCry, nguy cơ tấn công APT

Bkav xin khuyến cáo đơn vị tải công cụ quét, kiểm tra lỗ hổng tại Bkav.com.vn/Tool/CheckWanCry.exe và cập nhật bản vá theo hướng dẫn.

Để phòng ngừa nguy cơ mã độc tấn công, nên sao lưu dữ liệu thường xuyên, cập nhật bản vá cho hệ điều hành. Chỉ mở các file văn bản nhận từ Internet trong môi trường cách ly Safe Run và cài phần mềm diệt virus thường trực trên máy tính để được bảo vệ tự động.

Trong trường hợp cần sự trợ giúp, xin liên hệ:

Bộ phận an ninh mạng – Công ty Cổ phần Bkav

Tòa nhà Bkav, đường Dương Đình Nghệ, Yên Hòa, Cầu Giấy, Hà Nội



Di động: 0904 768 799 (Nguyễn Tuấn Anh)

Email: Security@bkav.com

Xin trân trọng cảm ơn./.

Nơi nhận:

- Như kính gửi;
- Lưu: VP.

CÔNG TY CỔ PHẦN BKAV



Giám đốc

Lê Thanh Nam

