UBND TỈNH PHÚ YÊN
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 228 /SGDĐT-VP

V/v thông báo các phương thức tấn công khai thác hệ thống mới của tin tặc

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

Phú Yên, ngày 17 tháng 5 năm 2017

Kính gửi:
- Phòng GDĐT các huyện, thị xã, thành phố;
- Các đơn vị trực thuộc Sở.

Ngày 17/5/2017, Sở Giáo dục và Đào tạo nhận được Công văn số 399/STTTT-DL&DV.VT, ban hành ngày 16/5/2017 của Sở Thông tin và Truyền thông về việc các phương thức tấn công khai thác hệ thống mới của nhóm tin tặc Shadow Brokers.

Sở Giáo dục và Đào tạo thông báo đến các đơn vị biết để có giải pháp phòng ngừa hữu hiệu sự xâm nhập, tấn công của tin tặc trên hệ thống máy vi tính.

(Đính kèm Công văn số 399/STTTT-DL&DV.VT, 16/5/2017 của Sở Thông tin và Truyền thông).

Sở Giáo dục và Đào tạo thông báo đến phòng Giáo dục và Đào tạo các huyện, thị xã, thành phố và các đơn vị trực thuộc Sở, đề nghị các đơn vị triển khai./.

Nơi nhận:
- Như trên;
- Website Sở;
- Lưu: VT.

TL. GIÁM ĐỐC
KT. CHÁNH VĂN PHÒNG
PHÓ CHÁNH VĂN PHÒNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH PHÚ YÊN

Lê Thị Lập

UBND TỈNH PHÚ YÊN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 399/STTTT-DL&DV.VT

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

Phú Yên, ngày 16 tháng 5 năm 2017

V/v các phương thức tấn công khai thác hệ thống mới của nhóm tin tặc Shadow Brokers

Kính gửi:
- Các Sở, Ban, Ngành, Đoàn thể;
- UBND các huyện, thị xã, thành phố;
- Phòng VHTT các huyện, thị xã, thành phố

Theo công bố của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam, nhóm tin tặc có tên gọi là Shadow Brokers đã đánh cắp được một bộ công cụ gián điệp tấn công hệ thống nhằm khai thác dữ liệu của Cơ quan An ninh mạng quốc gia Hoa Kỳ (NSA). Do không đạt được thỏa thuận về tài chính để đánh đổi bộ công cụ, nhóm tin tặc Shadow Brokers đã tung lên mạng thông qua website chuyên về mã nguồn mở Github. Bộ công cụ bao gồm các chương trình nhị phân đã được biên dịch để khai thác bất kỳ hệ thống nào sử dụng các phiên bản của hệ điều hành Windows (trừ Windows 10 và Windows Server 2016) thông qua các lỗ hổng chưa được khai thác. Các phương thức tấn công khai thác dữ liệu hệ thống được đưa ra như sau:

- Một trong các công cụ Hacking được công bố gọi là Eternalromance, chứa một giao diện dễ sử dụng và khai thác hệ thống Window thông qua các cổng TCP 445 và 139. Các lỗ hổng của hệ điều hành Window được công bố gồm: EternalBlue (MS17-010), EmeraldThread (MS10-06), EternalChampion (CVE-2017-0146 và CVE-2017-0147), ErraticGopher (lỗ hổng trên Windows Vista - không được hỗ trợ), EsikmoRoll (MS14-068), EternalRomance (MS17-010), EducatedScholar (MS09-050), EternalSynergy (MS17-010), Eclipsed Wing (MS08-067).

- Bên cạnh đó, nhóm tin tặc Shardow Brokers còn khai thác lỗ hổng zero-day (CVE-2016-6366) ExtraBacon qua giao thức SNMP - giao thức tầng ứng dụng trong phần mềm Cisco ASA cho phép tin tặc không cần xác thực từ xa để khởi động lại hệ thống hoặc thực thi mã tùy ý, từ đó chiếm quyền kiểm soát thiết bị. Một hành vi tấn công hệ thống của Cisco cũng được khai thác thông qua tệp tin giải mã lưu lượng mạng riêng ảo (VPN) Cisco PIX và cấy mã độc vào bo mạch chủ firmware nhằm che dấu hành vi và xóa dấu vết.

Để phòng tránh các rủi ro mất an toàn thông tin mạng liên quan đến các công cụ tấn công của nhóm tin tặc Shadow Broker, Sở Thông tin & Truyền thông Phú Yên khuyến cáo các đơn vị sử dụng các biện pháp sau:

- Đối với hệ thống sử dụng hệ điều hành Windows (từ Windows Server 2000 tới Windows Server 2012, Windows XP, Windows Vista, Windows 7, Windows 8,...) nhanh chóng rà soát và cập nhật các bản vá lỗi được cảnh báo trên tại website chính thức của Mircosoft;

- Đối với hệ thống sử dụng các thiết bị của Cisco, cập nhật các bản vá lỗi liên quan đến lỗ hổng zero - day (CVE-2016-6366). Để bảo vệ dữ liệu an toàn, máy tính nên được bảo vệ đằng sau Router hoặc Firewalls. Trang bị các hệ thống phòng chống tấn công mạng như IPS/IDS, Firewalls...;

- Cập nhật phiên bản mới nhất của các chương trình diệt Virus để phát hiện và xử lý các mã thực thi do tin tặc tấn công vào hệ thống;

- Thực hiện sao lưu dữ liệu định kỳ: Sử dụng các ổ đĩa lưu trữ ngoài như ổ cứng cắm ngoài, ổ đĩa USB để lưu trữ các dữ liệu quan trọng trong máy tính. Sau khi sao lưu xong đưa ra cất giữ riêng và không kết nối vào internet.

Do tính chất phương thức tấn công trên rất nghiêm trọng và để phòng ngừa có hiệu quả, hạn chế tối đa khả năng bị tấn công vào trong máy tính. Sở Thông tin và Truyền thông đề nghị các Sở, Ban, Ngành và địa phương thông tin kịp thời về Trung tâm Dữ liệu & DV.VT – Sở Thông tin và Truyền thông và PA81 – Công an Tỉnh./.

Nơi nhận:
- Như trên;
- Tỉnh ủy (b/c);
- UBND tỉnh (b/c);
- Ban Giám đốc Sở;
- P.CNTT;
- Lưu: VT, TT.DL&DV.VT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XHCN VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH PHÚ YÊN

Lê Tỷ Khánh