BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU
KHẨN CẤP MÁY TÍNH VIỆT NAM

Số: 123 /VNCERT – ĐPƯC
V/v các phương thức tấn công khai thác hệ thống mới của nhóm tin tặc Shadow Brokers.

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

Hà Nội, ngày 24 tháng 4 năm 2017

Kính gửi:

- Các đơn vị chuyên trách về CNTT, ATTT Văn phòng Trung ương Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Văn phòng Chính phủ;
- Các đơn vị chuyên trách về CNTT các Bộ, Ngành;
- Các đơn vị thuộc Bộ Thông tin và Truyền thông;
- Các Sở Thông tin và Truyền thông;
- Các Tập đoàn kinh tế; Tổng công ty nhà nước; Tổ chức tài chính và ngân hàng; Các doanh nghiệp hạ tầng Internet, Viễn thông, Điện lực, Hàng không, Giao thông vận tải.

Ngày 14 tháng 4 năm 2017, nhóm tin tặc có tên gọi Shadow Brokers tuyên bố 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. Mục tiêu của các công cụ tấn công này nhằm vào các tổ chức tiền tệ, ngân hàng lớn, phần đông có trụ sở tại khu vực Trung Đông như UAE, Kuwait, Qatar, Palestine và Yemen. Theo báo cáo đánh giá của các chuyên gia an toàn thông tin mạng cho thấy điều này có gây ra nguy cơ mất an toàn thông tin trên diện rộng đa quốc gia, trong đó có Việt Nam.

Thực hiện thông tư số 27/2011/TT-BTTTT ngày 04/10/2011 của Bộ Thông tin và Truyền thông quy định về điều phối các hoạt động ứng cứu sự cố

mạng Internet Việt Nam, nhằm ngăn chặn sự lây lan và giảm thiểu rủi ro cho các đơn vị nắm giữ hệ thống thông tin quan trọng, đơn vị và doanh nghiệp sử dụng giao dịch thanh toán trực tuyến và người dùng Internet, Trung tâm VNCERT yêu cầu các cơ quan, doanh nghiệp cần chú ý và tăng cường công tác bảo đảm an toàn thông tin mạng để phòng ngừa sự cố có thể xảy ra.

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 Shardow Broker đưa ra, Trung tâm VNCERT khuyến cáo các đơn vị, doanh nghiệp 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.

Để giúp các cơ quan chức năng theo dõi, phân tích và kịp thời phản ứng nhanh với các phương thức tấn công mới, ngay khi phát hiện sự cố và không có khả năng xử lý thông báo ngay về:

Đầu mối Điều phối ứng cứu sự cố Quốc gia:

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT

- Địa chỉ: Tầng 5, Tòa nhà 115 Trần Duy Hưng, Cầu Giấy, Hà Nội;

- Điện thoại: 04 3640 4423 số máy lẻ 112;

- Đường dây nóng: 0934 424 009;

- Hòm thư điện tử tiếp nhận báo cáo sự cố: ir@vncert.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Cục ATTT, Cục BĐTW, VNNIC, NEAC;
- Giám đốc (để b/c);
- Các phòng, CN;
- Lưu VT, ĐPƯC.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Nguyễn Khắc Lịch