|  |  |
| --- | --- |
| UBND TỈNH ĐIỆN BIÊN **SỞ THÔNG TIN VÀ TRUYỀN THÔNG**  Số: 239/STTTT-TTCNTT  V/v cảnh báo và xử lý lỗ hổng liên quan đến trình soạn thảo văn bản MS Word | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập - Tự do - Hạnh phúc**  *Điện Biên, ngày 28 tháng 4 năm 2017* |

|  |  |
| --- | --- |
| Kính gửi: | - Các Sở, ban, ngành, đoàn thể tỉnh;  - UBND các huyện, thị xã, thành phố; |

Theo cảnh báo của Ban Cơ yếu Chính phủ, Trung tâm An ninh mạng BKIS đã ghi nhậnmột lỗ hổng Zero-Day trên phần mềm soạn thảo văn bản Microsoft Word ảnh hưởng tới toàn bộ các phiên bản Windows. Người dùng máy tính Việt Nam đứng trước nguy cơ bị tấn công diện rộng, bởi hầu hết các máy tính đều cài đặt hệ điều hành Windows và sử dụng phần mềm soạn thảo văn bản Microsoft Word.

Thực hiện quy định tại Thông tư 27/2011/TT-BTTTT ngày 04/10/2011 của Bộ Thông tin và Truyền thông về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam. Sở Thông tin và Truyền thông đề nghị Sở, ban, ngành tỉnh; UBND các huyện, thị xã, thành phố cầnlưu ý và tăng cường công tác tuyên truyền đến cán bộ, CCVC, người dùng máy tính trong cơ quan để phòng ngừa sự cố xảy ra, cụ thể:

**1. Thông báo về lỗ hổng CVE-2017-0199**

Khai thác lỗi phần mềm soạn thảo văn bản Microsoft Office bắt đầu bằng việc gửi một email hoặc các trang chia sẻ tài liệu giả mạo, đính kèm tệp tin Word độc hại chứa OLE2link (Windows Object Linking and Embedding). Khi người dùng mở tệp tin, mã khai thác sẽ được thực thi và kết nối tới máy chủ từ xa do tin tặc kiểm soát. Tại đây mã khai thác tải về một tệp tin ứng dụng HTML (HTA) độc hại giả mạo tệp tin tài liệu RTF (Rich Text Format) của Microsoft.

Tệp tin HTA sau đó tự động thực thi trên máy nạn nhân, tải thêm các mã độc khác về để chiếm quyền kiểm soát máy tính nạn nhân, đồng thời đóng tập tin Word lại

Theocác nhà nghiên cứu bảo mật FireEye một hãng bảo mật danh tiếng: *"Cuộc tấn công liên quan đến một diễn viên gửi mail tài liệu Microsoft Word có nhúng OLE2link đến một người dùng khác. Khi người dùng mở tài liệu, winword.exe sẽ đưa ra yêu cầu HTTP đến máy chủ từ xa để lấy ra tập tin .hta độc hại, xuất hiện dưới dạng file RTF giả mạo. Ứng dụng HTA của Microsoft tải và thực thi mã độc hại. Trong cả hai tài liệu được quan sát, tập lệnh độc hại đã dừng quá trình của winword.exe, tải thêm payload và nạp một tài liệu khác để "nhử" người dùng. Quá trình winword.exe ban đầu được chấm dứt để ẩn thông báo nhắc nhở người dùng được tạo ra từ OLE2link".*

Hãng Microsoft đã biết đến lỗ hổng sau khi được các chuyên gia thông báo về các cuộc tấn công khai thác lỗ hổng chưa được vá từ tháng 1/2017. Đã đượcMITRE Corporationđặt mã tên quốc tế: **CVE - 2017-0199**

**2. Các nguy cơ của Lỗ hổng CVE - 2017-0199**

Các phiên bản bị ảnh hưởng bao gồm: Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1.

Do đó có thể qua mặt các hệ thống dò quét mã độc.Khi máy tính bị nhiễm mã độc cho phép tin tặc từ xa kiểm soát máy tính nạn nhân, tấn công leo thang sang máy chủ (Server). Theo đánh giá của Bkav, đây là một lỗ hổng nghiêm trọng dễ bị lợi dụng để tiến hành các cuộc tấn công APT bởi kịch bản tấn công APT thường sử dụng là gửi email đính kèm file văn bản chứa mã độc *"Với tâm lý cho rằng file văn bản thì an toàn, rất nhiều người sử dụng đã mắc lừa và mở file đính kèm, sau đó máy tính đã bị nhiễm mã độc".*

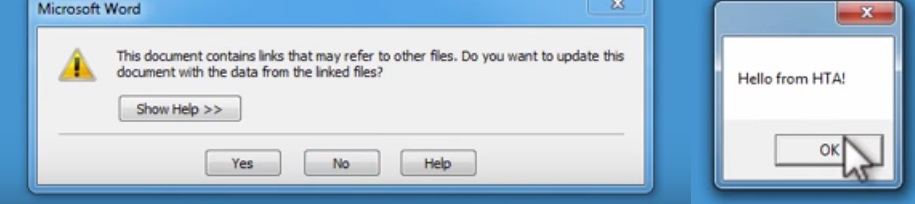
**3. Các phương pháp lây lan chủ yếu của mã độc**

-Tin tặc gửi tập tin đính kèm quathư điện tử, khi người dùng mở tập tin thì mã độc sẽ tự động lây nhiễm vào máy tính người dùng.

- Tin tặc gửi tin nhắn chứa đường dẫn tải mã độc và yêu cầu người dùng tải về và cài đặt qua các ứng Chat trên mạng xã hội, gmail, yahoo...

- Khi người dùng cần tìm tài liệu tải các tập tin trên Internet, nên cẩn trọng kiểm tra xem tập tin tải về có an toàn hay không.

Ngoài ra máy tính có thể bị lây nhiễm thông qua đường khác như qua các thiết bị lưu trữ, quá trình cài đặt phần mềm không rõ nguồn gốc, sao chép dữ liệu từ máy bị nhiễm,...

Dấu hiệu nhận biết khi mở một tập tin Word mới tải về, sao chép từ máy tính và thiết bị lưu trữ khác sẽ có một bảng thông báo hoặc thông báo tương tự như sau:

**4. Biện pháp xử lý**

Để phòng ngừa loại mã độc này, Sở Thông tin và Truyền thông khuyến cáo các đơn vị xử lý một số biện pháp sau:

4.1. Phòng ngừa để hạn chế tối đa khả năng bị nhiễm mà độc

- Cài đặt và thường xuyên cập nhật cho hệ điều hành, phần mềm chống mã độc như: Bkav, Kapersky, Symantec, Avast, AVG, CMC,...

- Chú ý cảnh giác với các tập tin đính kèm, các đường liên kết ẩn được gửi đến thư điện tử người dùng, kể cả người dùng nội bộ.

- Thực hiện các biện pháp nhằm kiểm tra xác thực người dùng trên máy chủ gửi mail của đơn vị, tránh giả mạo người gửi từ nội bộ.

- Tắt các chế độ tự động mở, chạy tập tin đính kèm theo thư điện tử.

- Khi tải các tập tin từ trên Internet về nên cẩn trọng kiểm tra trước khi mở tập tin tại địa chỉ sau:**https://www.virustotal.com/**(lưu ý khi tải về KHÔNG được mở xem nội dung mới tiến hành kiểm tra).

4.2. Thực hiện cập nhật hệ điều hành, phần mềm

- Cập nhật các bản vá lỗi mới nhất ngay lập tức theo địa chỉ sau *(kiểm tra phiên hệ điều hành, phần mềm Word trước khi tải bản vá)*:

**https://portal.msrc.microsoft.com/en-US/security-guidance**

- Cán bộ chuyên trách Công nghệ thông tin của đơn vị cần thường xuyên theo dõi, tham khảo tin tức về lỗ hổng bảo mật hệ thống tại các địa chỉ sau:

<http://stttt.dienbien.gov.vn> hoặc <http://dic.gov.vn>

http://www.vncert.gov.vn/

https://whitehat.vn/

http://antoanthongtin.vn/

**5. Xử lý khi bị lấy nhiễm mã độc**

- Nhanh chóng ngắt kết nối mạng, khi thấy nghi ngờ, chưa có hướng xử lý.

- Sử dụng phần mềm bắt gói tin kiểm tra kết nối từ máy bị nhiễm kết nối với địa chỉ IP lạ qua giao thức HTTP như: Wireshark, SmartSniff, Currporta. Từ đó tìm ra tập tin chạy ngầm.

- Sử dụng phần mềm kiểm tra các tiến trình chạy cùng hệ điều hành: Process Explorer, Process monitor. Tiến hành dừng chạy tiến trình của mã độc.

- Cài đặt lại toàn bộ hệ thống, cài đặt phần mềm diệt Virus đồng thời thiết lập chế độ cập nhật phiên bản hệ điều hành tự động.

Sở Thông tin và Truyền thông giao Trung tâm Công nghệ thông tin và Truyền thông phối hợp, hỗ trợ các cơ quan, đơn vị theo dõi, phân tích, bóc gỡ và phản ứng nhanh chóng với các loại mã độc mới.

*Thông tin chi tiết đề nghị liên hệ:*

*Trung tâm Công nghệ thông tin và Truyền thông, điện thoại: 0215.6250.662 - 0946.560.568 (Đ/c Nguyễn mạnh Cường Phòng Kỹ thuật. Thư điện tử: ict@dic.gov.vn*

Trân trọng./.

|  |  |
| --- | --- |
| ***Nơi nhận:***  - Như trên;  - Lãnh đạo Sở (b/c);  - Các phòng chuyên môn Sở;  - Trung tâm CNTT&TT;  - BBT Website (đăng tải);  - Lưu: VT. | KT. GIÁM ĐỐC **PHÓ GIÁM ĐỐC**    **Vũ Anh Dũng** |