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

Số: 14 /VNCERT-ĐPƯC
V/v điểm yếu mới của hệ quản trị nội dung mã nguồn mở Joomla và hình thức tấn công mới vào các trang tin điện tử tại Việt Nam

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

Hà Nội, ngày 18 tháng 01 năm 2016

Kính gửi:

- Các Sở Thông tin và Truyền thông
- Các đơn vị chuyên trách về CNTT các Bộ Ngành
- Các doanh nghiệp ISP
- Các doanh nghiệp làm về An toàn thông tin.

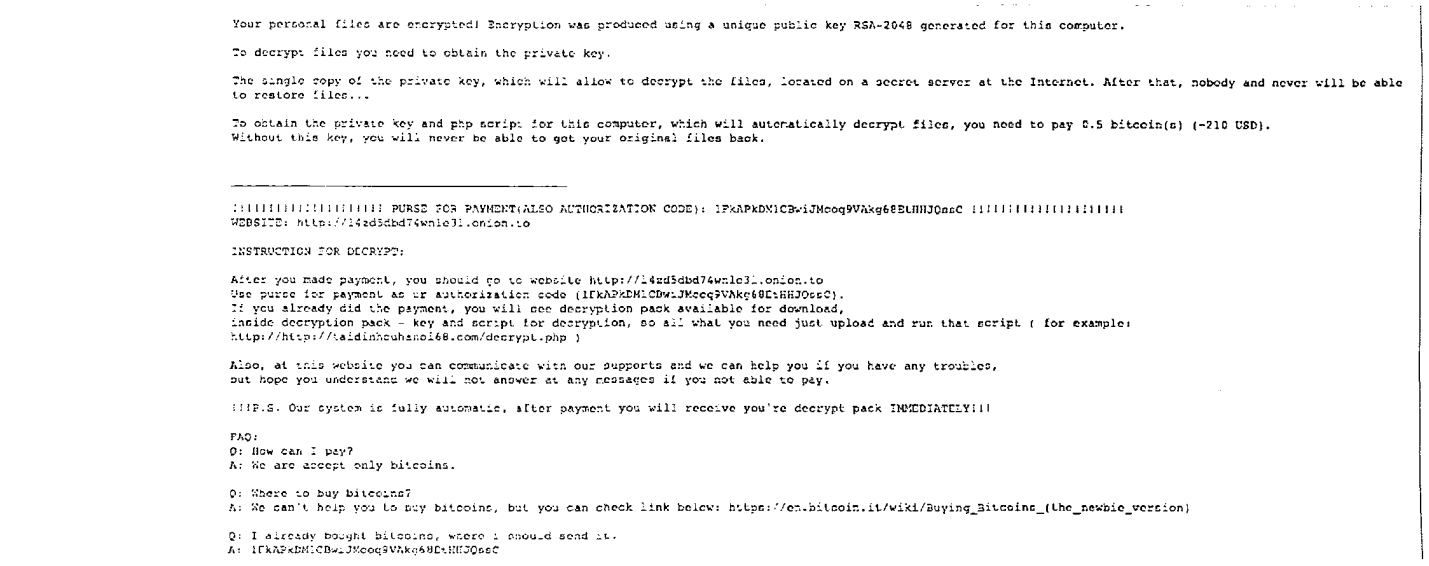
Trong thời gian gần đây, tại Việt Nam xuất hiện loại hình tấn công bằng cách khóa trang tin điện tử để đòi tiền chuộc sử dụng hình thức tấn công mã hóa tống tiền (ransomlock). Qua thông tin thu thập được của Trung tâm VNCERT, việc tăng vọt của hình thức tấn công này có liên quan đến điểm yếu của hệ quản trị nội dung Joomla được công bố gần đây.

Trước đây khi kiểm soát được một máy chủ web, tin tặc thường tiến hành thay đổi nội dung trang web, cài đặt các trang lừa đảo, cài đặt các đường liên kết đến mã độc hoặc thiết lập các cửa hậu phục vụ cho trộm cắp thông tin, phát tán thư rác hay tấn công từ chối dịch vụ. Các sự cố này thường không gây thiệt hại nhiều cho các chủ sở hữu trang tin điện tử, mà nạn nhân bị thiệt hại nhiều là người dùng và các tổ chức bị tấn công, lừa đảo, chính vì vậy, nhiều chủ sở hữu các trang tin điện tử không thực sự hợp tác với các cơ quan chức năng, các doanh nghiệp ISP để xử lý. Nhưng với loại hình tấn mã hóa trang tin điện tử để đòi tiền chuộc mới, tin tặc lại hướng trực tiếp vào người chủ trang tin điện tử, với mục tiêu làm cho trang tin điện tử bị tê liệt vì bị mã hóa nội dung và người sở hữu trang tin điện tử phải trả tiền cho tin tặc nếu muốn trang tin điện tử hoạt động trở lại.

1. Tình hình khai thác lỗ hổng và thủ đoạn tấn công mã hoá dữ liệu

Điểm yếu bảo mật mới nhất của Joomla đã được các nhà phát triển Joomla xác nhận có mã là CVE-2015-8562 đây là một điểm yếu Zero-day, với các phiên bản Joomla bị ảnh hưởng là từ V1.5.0 đến V3.4.5, điểm yếu này cho phép tin tặc thực thi lệnh các đoạn mã độc từ xa với đầy đủ các quyền. Hiện tại Joomla đã ban hành bản vá, tuy nhiên ngay khi điểm yếu này được tiết lộ thì trên Internet, mã khai thác cũng đã xuất hiện, theo ghi nhận của nhiều tổ chức

thì các tấn công khai thác điểm yếu này cũng tăng lên. Mức độ nguy hiểm của điểm yếu này tăng lên khi đã có ghi nhận xu hướng tin tặc thực hiện tấn công nhằm mục đích cài đặt các cửa hậu vào hệ thống trước khi quản trị cập nhật bản vá, chính vì vậy ngay cả cập nhật bản vá, trang tin điện tử vẫn bị tấn công và mã hóa dữ liệu. Ở Việt Nam, cũng đã ghi nhận một số trang tin điện tử tấn công và mã hóa tài liệu với nội dung hiển thị đòi tiền chuộc mà tin tặc để lại trên trang web bị tấn công.


Your personal files are encrypted! Encryption was produced using a unique public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow to decrypt the files, located on a secret server at the Internet. After that, nobody and never will be able to restore files...

To obtain the private key and php script for this computer, which will automatically decrypt files, you need to pay 0.5 bitcoin(s) (~210 USD).
Without this key, you will never be able to get your original files back.

!!!!!!!!!!!!!!!!!!!! PURSE FOR PAYMENT(ALSO AUTHORIZATION CODE): 1FkAPkDM1CBwiJMcoq9VAkg68BLHHJQnsC !!!!!!!!!!!!!!!!!!!!
WEBSITE: http://l4zd5dbd74wnle3l.onion.to

INSTRUCTION FOR DECRYPT:

After you made payment, you should go to website http://l4zd5dbd74wnle3l.onion.to
Use purse for payment as ur authorization code (1FkAPkDM1CBwiJMcoq9VAkg68EtHHJQnsC).
If you already did the payment, you will see decryption pack available for download,
inside decryption pack - key and script for decryption, so all what you need just upload and run that script (for example:
http://http://taidinhcuhanoi68.com/decrypt.php)

Also, at this website you can communicate with our supports and we can help you if you have any troubles,
but hope you understand we will not answer at any messages if you not able to pay.

!!!P.S. Our system is fully automatic, after payment you will receive you're decrypt pack IMMEDIATELY!!!

FAQ:
Q: How can I pay?
A: We are accept only bitcoins.

Q: Where to buy bitcoins?
A: We can't help you to buy bitcoins, but you can check link below: https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)

Q: I already bought bitcoins, where i should send it.
A: 1FkAPkDM1CBwiJMcoq9VAkg68EtHHJQnsC

Hình 1: Hình ảnh trang tin điện tử bị tấn công, hiển thị thông điệp đòi tiền chuộc

Qua phân tích từ các chuyên gia của VNCERT cho thấy nhiều khả năng khi khai thác thành công lỗ hổng này hay bất kỳ lỗ hổng nào của ứng dụng tin tặc có thể kiểm soát được toàn bộ nội dung trang tin điện tử. Và việc kiểm soát, tấn công chiếm quyền điều khiển thông qua lỗ hổng, điểm yếu của ứng dụng web hoàn toàn có thể được tin tặc kết hợp thủ đoạn tấn công mã hoá dữ liệu để đòi tiền chuộc từ chủ sở hữu trang tin điện tử.

2. Những nguy cơ tiềm ẩn và trách nhiệm của các tổ chức liên quan

Sự cố tấn công này cho thấy tin tặc đã có xu hướng tấn công từ lợi dụng trang tin điện tử làm bàn đạp sang hình thức tấn công có tính chất phá hoại cao hơn, thêm vào đó việc lợi dụng các điểm yếu Zero-day để tranh thủ khai thác và cài sẵn các cửa hậu cho thấy các loại hình tấn công mạng đã có sự dịch chuyển.

Với các trang tin điện tử bị tấn công theo hình thức này thì các đơn vị, doanh nghiệp sẽ bị mất hết dữ liệu, dẫn đến sẽ phải trả tiền chuộc hoặc xây dựng lại từ đầu các nội dung. Điều này gây thiệt hại cho các nguồn lực của doanh nghiệp và của xã hội.

Việc khai thác điểm yếu của Joomla, một hệ thống quản trị nội dung do chính các nhà cung cấp dịch vụ lưu trữ hoặc đơn vị chịu trách nhiệm quản trị máy chủ, ứng dụng cài đặt, người dùng không thể chủ động cập nhật, do vậy các doanh nghiệp cung cấp dịch vụ lưu trữ hoặc hoặc đơn vị chịu trách nhiệm quản trị máy chủ, ứng dụng phải có trách nhiệm trong việc nhanh chóng vá các lỗ hổng này.

3. Yêu cầu thực hiện lệnh điều phối

Căn cứ Thông tư số 27/2011/TT-BTTTT ngày 04/10/2011 Quy định về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam và xét thấy tính chất nghiêm trọng điểm yếu của hệ quản trị nội dung Joomla và xu hướng tấn công mới của tội phạm, Trung tâm VNCERT yêu cầu Quý đơn vị thực hiện các công việc sau:

a) Yêu cầu chung

- Kiểm tra, rà soát các máy chủ sử dụng hệ quản trị nội dung Joomla đang sử dụng (nếu có), và cập nhật ngay bản vá cho các phiên bản Joomla bị ảnh hưởng.

- Chủ động sao lưu dữ liệu cho các máy chủ đặc biệt là các máy chủ web có khả năng bị tấn công, đảm bảo an toàn cho các bản sao lưu, tuyệt đối không để các bản sao lưu dữ liệu trên cùng một máy chủ hoặc trên các máy chủ có kết nối mạng.

- Thường xuyên theo dõi, kiểm tra để có phương án xử lý kịp thời khi có các điểm yếu được phát hiện, tiến hành cập nhật các bản vá cũng như đưa ra phương án giảm thiểu thiệt hại trong thời gian sớm nhất.

- Tiếp tục thực hiện cảnh báo tới các đơn vị nằm trong phạm vi trách nhiệm và địa bàn hoạt động của đơn vị mình.

b) Yêu cầu đối với các doanh nghiệp ISP có cung cấp dịch vụ lưu trữ

- Kiểm tra, rà soát các máy chủ sử dụng hệ quản trị nội dung Joomla đang sử dụng (nếu có), và cập nhật ngay bản vá cho các phiên bản Joomla bị ảnh hưởng.

- Chủ động sao lưu dữ liệu của các máy chủ hoặc khuyến nghị khách hàng thực hiện sao lưu dữ liệu định kỳ tùy theo mức độ quan trọng của dữ liệu. Tuyệt đối không để các bản dữ liệu sao lưu trên cùng một máy chủ hoặc trên các máy chủ có kết nối mạng.

- Thường xuyên theo dõi, kiểm tra để có phương án xử lý kịp thời khi có các điểm yếu được phát hiện, tiến hành cảnh báo cho khách hàng cũng như cập nhật các bản vá hay đưa ra phương án xử lý giảm thiểu thiệt hại trong thời gian sớm nhất.

4. Đầu mối điều phối ứng cứu quốc gia

Báo cáo về Trung tâm VNCERT tình hình xử lý hoặc sự cố tấn công vào các máy chủ của đơn vị và các khó khăn trong việc triển khai các giải pháp đảm bảo an toàn thông tin để xây dựng phương án xử lý cũng như cảnh báo rộng rãi cho cộng đồng trước ngày 30/1/2016 bằng đường công văn hoặc thư điện tử theo địa chỉ như sau:

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam:

- Địa chỉ: 18 Nguyễn Du – Hai Bà Trưng – Hà Nội;
- Điện thoại: 04 3640 4423;
- Điện thoại di động: 0934424009;
- Hòm thư điện tử tiếp nhận báo cáo sự cố: ir@vncert.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ Trưởng Nguyễn Bắc Son (để b/c);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Giám đốc (để b/c);
- Lưu: VT, ĐPƯC (1), HHT (3).

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