CẢNH GIÁC EMAIL MẠO DANH VNNIC PHÁT TÁN VIRUS!

Khoảng

Khoảng hai ngày nay, xuất hiện hàng loạt email giả mạo địa chỉ mail của Trung tâm Internet Việt Nam (VNNIC) gửi đi các thông báo cảnh báo virus, nhưng bản thân các bức mail này lại chứa mã độc trong file đính kèm nhằm tấn công người dùng.

Nội dung email như sau:

"Trung tâm internet Việt Nam (VNNIC) xin thông báo các cơ quan, gần đây chúng tôi phát hiện có một loại virus nguy hiểm giả danh địa chỉ email phát tán khiến 5.500 máy tính tại các cơ quan nhà nước bị nhiễm... Chúng tôi xin gửi kèm danh sách email nguy hiểm trong file đính kèm"
Địa chỉ gửi từ bức mail có nội dung như trên đề rõ là VNNIC , nhưng thực tế, đây là một email giả mạo!

File đính kèm mà bức mail giả mạo giải thích là "danh sách email nguy hiểm" thực chất lại là một virus có tên Dropper.Mdrop.AC.

Hình ảnh bức mail giả mạo thông báo của VNNIC để phát tán Virus tấn công người dùng
Ngay sau khi nhận được các thông tin thông báo về loại hình phát tán virus như trên, VietNamNet đã có liên hệ trực tiếp với VNNIC để làm rõ sự việc.

Các khuyến cáo khi tương tác với email có file đính kèm:

- Cảnh giác với các file đính kèm mà mình không yêu cầu, thậm chí các file đó được gửi từ người quen – Vì một email có địa chỉ người gửi là quen biết không có nghĩa là nó được gửi từ chính người đó. Nếu có thể, hãy kiểm tra tính xác thực từ phía người gửi trước khi mở file đính kèm.

Cẩn thận với các thông điệp từ các ISP, các hãng phần mềm, các công ty Game online,… yêu cầu mở hay cài đặt các file đính kèm theo. Các công ty, tổ chức này không gửi phần mềm qua email

mà luôn yêu cầu tải trực tiếp từ web site chính thức của họ.

- Lưu và quét bất cứ file đính kèm nào trước khi mở chúng

- Nếu phải mở một file đính kèm trước khi bạn có thể xác thực nguồn gốc, làm các bước sau đây:
(1) Đảm bảo phần mềm chống virus được cập nhật gần nhất.

(2) Lưu file vào máy tính hoặc một ổ đĩa nào đó.

(3) Quét file đó một cách thủ công sử dụng phần mềm diệt virus.

(4) Mở file.
Tắt tính năng tự động tải các file đính kèm của các phần mềm đọc mail.

- Xem xét thêm các biện pháp khác – Lọc các kiểu file đính kèm sử dụng các tùy chọn giới hạn kiểu file đính kèm của phần mềm email hoặc sử dụng một firewall.
Nguồn: VNCERT

Ông Phạm Việt Anh - Trưởng phòng Kỹ thuật điều hành của VNNIC khẳng định: "Đây là một dạng giả mạo địa chỉ email của VNNIC để phát tán virus".

Đại diện VNNIC cũng nhận định, loại hình giả mạo địa chỉ email VNNIC để phát tán mã độc tấn công người dùng có thể có nhiều hình thức khác chứ không chỉ có một nội dung cụ thể như đã nêu ở trên.

Vì thế ông Việt Anh nhấn mạnh: "VNNIC chưa bao giờ gửi đi các email liên quan đến cảnh báo virus! Trước giờ các email được gửi đi từ VNNIC chủ yếu nằm trong chức năng của trung tâm là liên quan đến vấn đề tên miền như Thông báo hết hạn duy trì tên miền, hoặc email liên hệ với các chủ thể tên miền khi có yêu cầu thay đổi, thắc mắc.v.v."

Ngay sau khi nhận được thông tin từ các khách hàng bị nhiễm mã độc do nhận được các mail giả mạo như trên, VNNIC đã có thông báo gửi đến Trung tâm VNCERT (Bộ BCVT), Trung tâm BKIS (ĐH Bách khoa HN) và VietNamNet để đưa ra các thông tin xử lý kịp thời và cảnh báo người dùng.

Ông Đỗ Ngọc Duy Trác - Trưởng phòng nghiệp vụ của VNCERT đưa ra khuyến cáo: "Việc hacker giả mạo địa chỉ phần gửi đi (from) trong email rất dễ dàng, vì thế người dùng cần hết sức cẩn thận trước những bức email có nội dung tương tự (có địa chỉ gửi đi từ VNNIC và có file đính kèm)."

"Nếu phát hiện các sự cố tương tự, mong mọi người thông báo lại với VNCERT thông qua email ir@vncert.vn hoặc qua số điện thoại 04.9445510. Một việc nên làm nữa là các bạn hãy cập nhật trương trình antivirus đang có và luôn cảnh giác với các thủ đoạn tương tự. Hacker có thể giả mạo địa chỉ email từ các công ty, tổ chức khác..., thậm chí cả VNCERT. Đối với Trung tâm VNCERT, chúng tôi không bao giờ gửi email đính kèm file đến người dùng và mọi email nghiệp vụ đều sử dụng chữ ký điện tử tương thích với chuẩn OpenPGP để phía nhận có thể kiểm tra tính xác thực".

Hiện vẫn chưa có các thống kê về thời điểm chính xác loại virus trên được tung lên mạng, số nạn nhân bị lây nhiễm cũng như mức độ nguy hiểm của loại virus này. Tuy nhiên, số máy tính bị lây nhiễm có thể khá lớn do thông tin từ VNCERT cho thấy hacker phát tán virus theo dạng spam mail - gửi thư rác số lượng lớn vào tất cả các đối tượng người dùng mà chúng có danh sách email.

Thế Phong