MỘT SỐ GỢI Ý PHÒNG TRÁNH CÁC CUỘC TẤN CÔNG PHISHING

ThS. Phan Trần Điền (*)

KS. Nguyễn Trí Đức (**)

1. Đặt vấn đề

Sự phát triển vượt bậc của ngành công nghệ thông tin trong những năm trở lại đây, đặc biệt là sự phát triển nhanh chóng của mạng internet, đã tạo cơ hội cho các cơ quan, doanh nghiệp, cá nhân giới thiệu thông tin của mình trên xa lộ thông tin, cũng như thực hiện các phiên giao dịch trực tuyến trên mạng internet ngày càng nhiều. Tuy nhiên, việc giao dịch trực tuyến trên mạng internet đã tạo ra những khe hở để hacker có thể đánh cắp thông tin của người dùng. Kỹ thuật đánh cắp thông tin thường được hacker sử dụng là hình thức tấn công giả mạo để lừa người dùng nhằm để lấy các thông tin nhạy cảm của người dùng khi tham gia giao dịch trực tuyến như: tài khoản, mật khẩu hay số thẻ tín dụng bằng cách giả mạo một tổ chức đáng tin cậy trong giao dịch điện tử như ngân hàng, các hệ thống thanh toán trực tuyến, hay các mạng xã hội phổ biến.

2. Tấn công Phishing

Phishing là việc xây dựng những hệ thống lừa đảo nhằm đánh cắp các thông tin nhạy cảm, như tên đăng nhập, mật khẩu hay thông tin về các loại thẻ tín dụng của người dùng. Phishing xuất hiện như một thực thể đáng tin cậy, một trang thông tin điện tử, eBay, Paypal, Gmail, hay các ngân hàng trực tuyến là những mục tiêu hướng đến của hình thức tấn công này. Phishing thường được thực hiện qua email, những tin nhắn nhanh và thường tập trung vào hướng lừa người dùng nhập các thông tin vào một form hay nhấp chuột vào một đường dẫn của website lừa đảo.

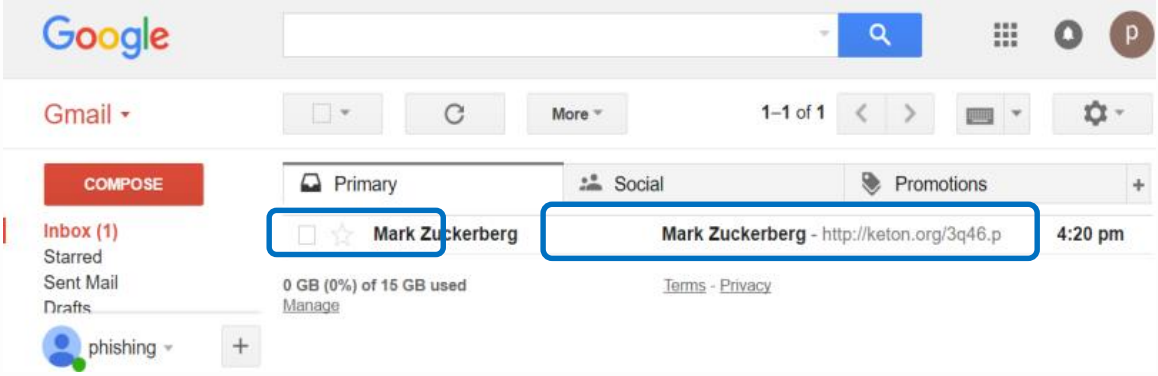
Các vụ tấn công Phishing giờ đây thường tập trung vào đối tượng các khách hàng thanh toán trực tuyến, bằng việc phát tán mã độc hoặc đường liên kết giả mạo để đánh cắp thông tin người dùng và sau đó thực hiện lệnh chuyển tiền qua nhiều tài khoản trung gian để xóa truy vết.

(*),(**) Giảng viên Khoa Đại cương, Học viện Cán bộ Thành phố Hồ Chí Minh

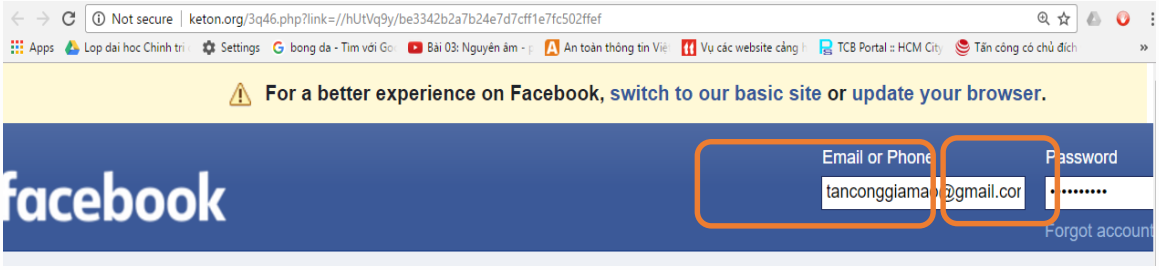
Phương thức phổ biến nhất trong các tấn công Phishing là mạo danh thông qua email. Hacker thường tạo email với phần địa chỉ có đuôi mạo danh từ những website đáng tin cậy và phổ biến như facebook.com hoặc apple.com. Người dùng rất dễ bị đánh lừa để nhấp chọn vào đường liên kết dẫn đến những website giả mạo do hacker dựng lên giống với website chính thống hoặc các form đăng nhập giả mạo. Khi người dùng nhập thông tin vào website giả mạo và form giả mạo, thông tin này sẽ được đánh cắp và bí mật gửi đến hacker. Ví dụ các bước tấn công giả mạo mạng xã hội Facebook như sau:

– Hacker tạo một tài khoản tấn công trên trang: http://z-shadow.co/

– Tạo địa chỉ email với phần địa chỉ có phần đuôi mạo danh từ những website đáng tin cậy hoặc phần địa chỉ là tên của các doanh nhân hoặc các công ty phổ biến như facebook, google, yahoo…

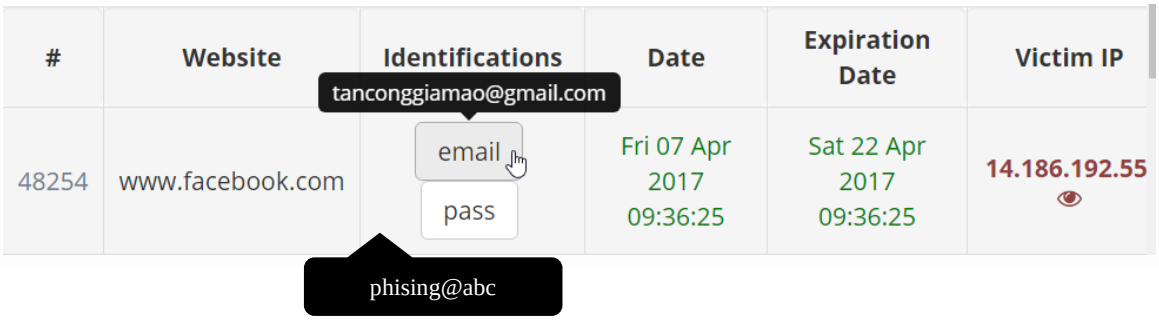


– Bên cạnh đó, các đường dẫn mạo danh với tên miền gần giống như facebook và được chèn thêm liên kết giả khiến cho người dùng bị đánh lừa và nhấp chuột vào. Có hai khả năng xảy ra: *Một là,* khi nhấp chuột vào đường liên kết vô tình kích hoạt mã độc được chèn sẵn vào đường dẫn mạo danh; *Hai là,* mở ra một website mạo danh chứa form đăng nhập giả mạo trang mạng xã hội facebook.



– Trong ví dụ minh họa này thông tin Username và Password đăng nhập vào Facebook sẽ gửi vào tài khoản được tạo trên trang http://z-shadow.co/. Hacker lấy

được tài khoản và mật khẩu facebook của người dùng khi đăng nhập vào form đăng nhập giả có giao diện giống trang mạng xã hội facebook.



3. Phòng tránh các cuộc tấn công Phishing.

Sau đây là một số gợi ý nhằm giúp người dùng có thể phòng tránh các cuộc tấn công Phishing như:

– Máy tính phải luôn được bảo vệ bằng các chương trình diệt virus.

– Đừng bao giờ tin vào một email chỉ dựa trên địa chỉ hoặc đuôi email của người gửi, bởi chúng hoàn toàn có thể bị giả mạo. Các tổ chức ngân hàng, tài chính hoặc giao dịch trực tuyến như Internet Banking không bao giờ yêu cầu người dùng nhập thông tin truy cập ở biểu mẫu ngay trong email gửi cho khách hàng.

– Cần cảnh giác với các đường dẫn đính kèm trong email, hạn chế nhấp chuột vào đường dẫn nếu có nghi ngờ và cần xem kỹ phần địa chỉ khi truy cập. Tuyệt đối không nhập các thông tin nhạy cảm vào các website không sử dụng giao thức bảo mật https.

– Các email chính thức từ các ngân hàng, tổ chức sẽ không bao giờ chứa các tập tin đính kèm. Vì tất cả các thông tin liên quan đến khách hàng (biểu mẫu, ứng dụng…) được giới thiệu trên trang web của ngân hàng, tổ chức.

– Theo dõi cẩn thận các SMS thông báo biến động số dư cũng như các mã OTP phát sinh bất thường. Nếu thấy có nguy cơ lừa đảo hãy báo ngay cho ngân hàng và yêu cầu khóa tài khoản tạm thời để bảo vệ tài khoản, ngăn chặn các giao dịch chuyển tiền bất hợp pháp.

– Chú ý các tin nhắn chứa mã yêu cầu truy cập tài khoản Facebook, Gmail,..., nếu thấy bất thường hãy tăng cường bảo mật.

– Tuyệt đối không truy cập các website khiêu dâm, vốn chứa nhiều rủi ro về bảo mật và các mã độc. Cần hạn chế lưu lại thông tin nhạy cảm (mật khẩu, tên truy cập...) vào các ứng dụng như trình duyệt web vì rất dễ bị xem lén.

Kiểu tấn công Phishing tập trung vào thành phần người dùng thiếu hiểu biết về cách phòng tránh hoặc sự nhẹ dạ của người dùng. Việc thực hiện kỹ thuật tấn công Phishing rất đơn giản, không yêu cầu hacker phải có kiến thức chuyên sâu về công nghệ thông tin, vì vậy số lượng các vụ tấn công bằng kỹ thuật này ngày càng tăng, để đối phó với việc này mỗi người cần có những kiến thức cơ bản để phòng tránh. Các cơ quan, tổ chức cần có những buổi tập huấn nhằm tạo nhận thức về những mối nguy hại có thể xảy đến cho người dùng và tăng cường những biện pháp kỹ thuật để hạn chế tấn công Phishing.

TÀI LIỆU THAM KHẢO

[1]. Nguyễn Minh Đức (2014), Phishing là gì? Và cách để bạn bảo vệ mình, Security daily. Địa chỉ: http://securitydaily.net/phishing-la-gi-va-cach-de-ban-bao-ve-minh/

[2]. TM (2016), các loại Phishing phổ biến nhưng nhiều người vẫn mắc bẫy, VNReview. Địa chỉ: http://vnreview.vn/tu-van-bao-mat/-/view_content/content/1914747/cac-loai-phishing-pho-bien-nhung-nhieu-nguoi-van-mac-bay

[3]. Lamle (2010), cách thức hoạt động của Phishing, quản trị mạng. Địa chỉ: https://quantrimang.com/cach-thuc-hoat-dong-cua-phishing-69841

[4]. Phúc Thịnh (2016), 10 chiêu thức hack có thể hack tài khoản Facebook, VNReview. Địa chỉ: http://vnreview.vn/tu-van-web/-/view_content/content/1831312/10-chieu-thuc-hacker-co-the-hack-tai-khoan-facebook