ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

LÊ THỊ THU HƯƠNG

CÁC LỪA ĐẢO TRÊN MẠNG MÁY TÍNH VÀ CÁCH PHÒNG TRÁNH

Ngành: Công nghệ thông tin
Chuyên ngành: Truyền dữ liệu và Mạng máy tính
Mã số:

LUẬN VĂN THẠC SỸ CÔNG NGHỆ THÔNG TIN

HƯỚNG DẪN KHAO HỌC: PGS. TS Trịnh Nhật Tiến

HÀ NỘI 2016

GIỚI THIỆU

Lừa đảo qua mạng (Social Engineering) được thực hiện chủ yếu dựa trên việc khai thác hành vi và tâm lý của người sử dụng Internet; Và các "lỗ hổng" trong hệ thống an ninh mạng máy tính. Được phân làm 2 nhóm:

1- Cố gắng đánh lừa mọi người gửi tiền trực tiếp cho kẻ lừa đảo (ví dụ: giả bộ gặp trục trặc).

2- Lừa đảo nhằm mục đích ăn cắp thông tin cá nhân và dữ liệu máy tính.

Một trong những hình thức lừa đảo qua mạng khá phổ biến là "phishing – lừa đảo giả dạng". Trong phần nghiên cứu này ta sẽ tập trung nghiên cứu vào hình thức lừa đảo giả dạng "***phishing".***

Chương 1 – LÝ THUYẾT CÁC DẠNG LỪA ĐẢO QUA MẠNG

1.1. KHÁI NIỆM LỪA ĐẢO GIẢ DẠNG

Lừa đảo giả dạng (phishing) là loại hình gian lận (thương mại) trên Internet, một thành phần của "Social Engineering – kỹ nghệ lừa đảo" trên mạng. Nguyên tắc của lừa đảo giả dạng là bằng cách nào đó "lừa" người dùng gửi thông tin nhạy cảm đến kẻ lừa đảo; các thông tin như tên, địa chỉ, mật khẩu, số thẻ tín dụng, mã thẻ ATM, số an sinh xã hội,… . Cách thực hiện chủ yếu là mô phỏng lại giao diện đăng nhập trang web của các website có thật, kẻ lừa đảo sẽ dẫn dụ nạn nhân điền các thông tin vào trang "dỏm" đó rồi truyền tải đến anh ta (thay vì đến server hợp pháp) để thực hiện hành vi đánh cắp thông tin bất hợp pháp mà người sử dụng không hay biết.

1.2. LỊCH SỬ LỪA ĐẢO GIẢ DẠNG

Từ "phishing", ban đầu xuất phát từ sự tương đồng giống với cách mà bọn tội phạm Internet đầu tiên sử dụng e-mail để nhử "lừa đảo-phish" cho mật khẩu và các dữ liệu tài chính từ một biển người sử dụng Internet.Thuật ngữ này được đặt ra trong năm 1996 khoảng thời gian của tin tặc kẻ mà đã ăn cắp tài khoản (account) của America Online (AOL) bằng cách lừa đảo mật khẩu từ việc những người dùng AOL không nghi ngờ.

Đến năm 1996, tài khoản bị hack đã được gọi là "lừa đảo-phish", và đến năm 1997, Phish là giao dịch tích cực giữa các hacker như một hình thức tiền tệ điện tử.

Qua thời gian, định nghĩa thế nào là một cuộc tấn công lừa đảo-phishing đã bị mờ đi và phát triển rộng hơn.

Do tỷ lệ thành công cao của những vụ lừa đảo, hiện nay nó được lan rộng thành lừa đảo giả dạng –phishing;

1.3. TỔNG HỢP VỀ MỘT SỐ TỔ CHỨC BỊ TẤN CÔNG LỪA ĐẢO GIẢ DẠNG

IMF (Quỹ Tiền tệ Quốc tế)

Tin tặc đã tiến hành các cuộc tấn công trước ngày 14/5/2011, khi Strauss-Kahn, cựu Tổng giám đốc IMF bị bắt tại New York. Cuộc tấn công xâm nhập vào máy chủ của Quỹ Tiền tệ Quốc tế (IMF) có thể do các tin tặc, làm việc cho chính phủ nào đó ở nước ngoài, thực hiện. Tin tặc đã đánh cắp số lượng lớn dữ liệu bao gồm email và nhiều tài liệu khác. Các dữ liệu của IMF rất nhạy cảm vì nó chứa rất nhiều thông tin bí mật về tình hình tài chính của nhiều quốc gia trên thế giới và nó có thể ảnh hưởng đến thị trường toàn cầu. Tuy nhiên, hiện vẫn chưa có thông tin rõ ràng về các tài liệu mà tin tặc đã đánh cắp.

Google

Hôm 1/6/2011, Google cho biết hãng phát hiện các cuộc xâm nhập đánh cắp hàng trăm tài khoản người dùng và mật khẩu Gmail. Trong số các tài khoản bị đánh cắp, có rất nhiều tài khoản của các quan chức chính phủ Mỹ, các quan chức ở khu vực châu Á, các nhà báo…

Sony

Vụ tấn công mạng nhằm vào hãng Sony Pictures có thể đi vào lịch sử như vụ xâm nhập mạng máy tính lớn nhất năm 2014. Các thông tin số an sinh xã hội, hộp thư điện tử và tiền lương của các ngôi sao và nhân viên của Sony, cũng như bản sao các bộ phim chưa phát hành đã bị tung lên mạng.

Nhiều người suy đoán Bắc Triều Tiên đứng sau vụ rò rỉ dữ liệu lớn này vì cuộc tấn công xảy ra vài ngày trước sự kiện ra mắt dự kiến của "**The Interview**", bộ phim hài về một vụ ám sát hư cấu của CIA nhằm vào nhà lãnh đạo Triều Tiên Kim Jong-un.

Chương 2. CÁC PHƯƠNG PHÁP LỪA ĐẢO GIẢ DẠNG

2.1. NHỮNG YẾU TỐ ĐỂ CUỘC TẤN CÔNG LỪA ĐẢO GIẢ DẠNG THÀNH CÔNG

2.1.1. Sự thiếu hiểu biết

Sự thiếu hiểu biết về hệ thống mạng và máy tính đã giúp cho các hacker khai thác những thông tin nhạy cảm. Đặc biệt đối với những người thường xuyên mua bán, thanh toán qua mạng thì cần phải hiểu rõ việc cung cấp credit card là rất quan trọng và biết được khi nào nên cung cấp, khi nào không.

2.1.2. Nghệ thuật đánh lừa ảo giác

Nghệ thuật của sự đánh lừa ảo giác chính là làm cho nạn nhân không còn phân biệt được đâu là thật đâu là giả. Kỹ thuật đánh lừa ảo giác sẽ tạo ra một trang web, hoặc một lá thư…những thứ mà ngày nào bạn cũng truy cập, nó giống nhau đến mức gần như người ta không thể phát hiện ra sự giả mạo.

2.1.3. Không chú ý đến những chỉ tiêu an toàn

Như đã nói ở trên, những cảnh báo thường bị người dùng bỏ qua, chính điều đó đã tạo điều kiện cho hacker tấn công thành công hơn. Người dùng cũng thường không chú ý đến những chỉ tiêu an toàn. Ví dụ khi bạn truy cập một website thanh toán trực tuyến, bạn phải hiểu những quy định an toàn của website kiểu này, như thông tin về giấy chứng nhận (Cerificate), nhà cung cấp, nội dung, và nhiều quy định khác. Windows thường nhận biết những quy định an toàn này, và nếu không đủ nó sẽ lập tức cảnh báo cho người sử dụng. Tuy nhiên, có một số người dùng cảm thấy phiền phức với những cảnh báo này và đã tắt chức năng này đi, vì thế mà họ dễ dàng trở thành nạn nhân.

2.2. NHỮNG PHƯƠNG THỨC CỦA LỪA ĐẢO GIẢ DẠNG

2.2.1. Thư điện tử và thư rác (Email and Spam)

Hacker sẽ tiến hành gửi hàng loạt các thư đến những địa chỉ email hợp lệ. Bằng những kỹ thuật và công cụ khác nhau, hacker tiến hành thu thập địa chỉ email trước. Hacker đã lợi dung việc này để gửi đi những lá thư có nội dung bên ngoài có vẻ hợp lệ. Những nội dung này thường có tính khẩn cấp, đòi hỏi người nhận thư phải cung cấp thông tin ngay lập tức. Hacker sử dụng giao thức SMTP kèm theo một số kỹ thuật để giả mạo trường "Mail From" khiến cho người nhận không có chút nghi ngờ nào.

2.2.2. Phát tán dựa trên các trang mạng (Web-based Delivery)

Một kỹ thuật tiếp theo của Phishing là dựa vào việc phát tán các website lừa đảo. Bạn thường thấy các website dạng như kiếm tiền online. Chúng yêu cầu bạn cung cấp các thông tin tài khoản ngân hàng để tiến hành trả tiền công. Bạn không ngần ngại gì khi đang chờ đợi số tiền công hậu hĩnh. Kết cuộc tiền công không thấy mà tiền trong tài khoản cũng không còn.

Một hình thức khác là khiêu khích sự tò mò của người dùng. Bằng cách chèn vào trang web những biển hiệu (banner) hoặc những dòng chữ (text) quảng cáo có ý khiêu khích sự tò mò của người dùng. Ví dụ như những hình ảnh khiêu dâm, những nội dung đang nóng. Kết quả sau khi click vào đó thì máy tính của bạn có thể bị nhiễm một loại virus malware nào đó, virus này sẽ phục vụ cho một cộng tấn công khác.

2.2.3. Mạng lưới trò chuyện trực tuyến và tin nhắn khẩn (Irc and Instant Messaging)

Bằng những kỹ thuật tấn công, những kẻ lừa đảo tiến hành gửi tin nhắn tức thì đến hàng loạt người dùng. Những nội dung được gửi thường có liên quan đến hàng loạt người dùng, và cũng lợi dụng vào trí tò mò của mọi người. Kỹ thuật tinh vi của kiểu lừa đảo này là giả dạng nick chat.

2.2.4. Các máy tính bị nhiễm phần mềm gián điệp (Trojaned Hosts)

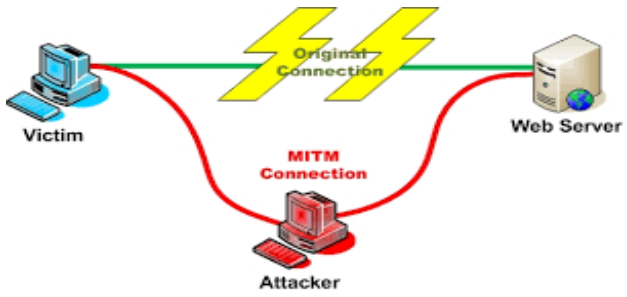
Một kiểu lừa đảo khác là lừa cho nạn nhân cài vào máy tính của mình một phần mềm gián điệp. Phần mềm gián điệp (trojan, keylog) này sẽ phục vụ cho một mục đích tấn công khác. Điển hình của công việc này là nạn nhân bị nhiễm trojan và trở thành một máy tính con trong một cuộc tấn công tổng thể trên diện rộng.

2.3. CÁC KIỂU LỪA ĐẢO GIẢ DẠNG

Căn cứ theo cách thức hoạt động, người ta phân loại những cuộc tấn công lừa đảo ra thành các loại sau.

2.3.1. Tấn công MITM

Ở kỹ thuật này, máy tính của kẻ tấn công được xem như là máy tính trung gian giữa máy tính của người dùng và website thật. Những kẻ tấn công dựng lên một máy tính trung gian để nhận dữ liệu của người dùng và chuyển nó cho website thật. Hoặc nhận dữ liệu của website thật rồi chuyển cho người dùng. Dữ liệu khi chuyển qua lại sẽ được lưu trữ lại tại máy tính của kẻ tấn công.



Tấn công MITM (Main-in-the-Middle)

Những kẽ tấn công ngoài việc dựng lên Proxy Server giả rồi dụ con mồi đến còn nghĩ đến việc tấn công vào các Proxy Server thật này để lấy dữ liệu.

Một cách khác để tấn công trong kỹ thuật này, là tìm cách làm lệch đường đi của gói dữ liệu. Một điểm cần lưu ý rằng, kỹ thuật tấn công này không phân biệt giao thức web là HTTP hay HTTPS.

2.3.2. Các cuộc tấn công gây rối URL (URL Obfuscation Attacks)

Làm rối URL (URL Obfuscation) là làm ẩn hoặc giả mạo URL xuất hiện trên các thanh địa chỉ một cách hợp pháp. Phương pháp tấn công làm rối URL sử dụng để làm cho cuộc tấn công và lừa đảo trực tuyến trở nên hợp pháp hơn. Một trang web xem qua thì hợp pháp với hình ảnh, tên tuổi của công ty, nhưng những liên kết trong đó sẽ dẫn đến những trang web của hacker. Việc giả mạo có thể nhắm đến những người dụng bất cẩn.

2.3.3. Tấn công XSS (Cross-Site Scripting Attacks)

Cross-Site Scripting hay còn được gọi tắt là XSS (thay vì gọi tắt là CSS là để tránh nhầm lẫn với CSS-Cascading Style Sheet của HTML) là một kĩ thuật tấn công bằng cách chèn vào các website động (ASP, PHP, CGI, JSP …). Các hacker sẽ chèn những đoạn script độc hại (thông thường là javascript hoặc HTML) vào website và sẽ được thực thi ở phía người dùng (trong trình duyệt của người dùng). Phụ thuộc vào mục đích của hacker, những đoạn Javascript được chèn vào để lấy những thông tin như:

+ Cookie; **+ Keylogging;** **+ Phishing.**

2.3.4. Tấn công ẩn (Hidden Attacks)

Attacker sử dụng các ngôn ngữ lập trình HTML, DHTML, hoặc ngôn ngữ dạng script khác để chèn vào trình duyệt của người dùng. Hoặc sử dụng các ký tự đặc biệt để đánh lừa người dùng. Những phương thức thường được attacker sử dụng là làm ẩn các frame. Các Frame sẽ được attacker làm ẩn đi trên trình duyệt của người dùng, qua đó attacker có thể chèn vào những đoạn mã độc. Một cách khác để tấn công là ghi đè nội dung trang web hoặc thay đổi hình ảnh trên trang web. Qua những nội dung bị thay đổi này, attaker sẽ chèn những đoạn mã độc hại vào đó.

Chương 3. PHƯƠNG PHÁP PHÒNG TRÁNH LỪA ĐẢO GIẢ DẠNG

3.1. PHÍA MÁY TRẠM

Ở phía khách hàng, khả năng bảo vệ chống lại lừa đảo có thể được tạo nên với:

3.1.1. Các doanh nghiệp bảo vệ máy tính để bàn

Lý tưởng nhất, hệ thống máy tính để bàn nên được cấu hình để sử dụng bảo vệ nhiều doanh nghiệp máy tính để bàn (ngay cả khi tính năng này sao lại bất kỳ dịch vụ bảo vệ nào trong phạm vi công ty), và có khả năng thực hiện các dịch vụ sau:

- Bảo vệ phòng chống Virus cục bộ (Anti-Virus)
- Tường lửa cá nhân
- IDS cá nhân
- Phát hiện Spyware
- Phòng chống thư rác (Anti-Spam) đối với từng cá nhân.

Ưu điểm : - Cài đặt dễ dàng.

- Bảo vệ chuyên sâu (Defense-in-Depth).
- Có sự kết hợp bảo vệ chéo (protection Overlapping).
- Nâng cao nhận thức và nâng cao cảnh giác phòng thủ mang tính nội bộ.

Nhược điểm: - Chi phí đặt mua cao (purchasing price).

- Cần gia hạn thuê bao (Subscription Renewals).
- Phức tạp và yêu cầu khả năng về quản lý.

3.1.2. Độ nhạy của thư điện tử (E-mail)

Chức năng này được nhúng một các không cần thiết (thường được để mặc định) được khai thác bởi các cuộc tấn công lừa đảo (cùng với sự tăng lên về xác suất của các

loại tấn công khác nhau). Nói chung, các ứng dụng phổ biến nhất cho phép người dùng tắt chức năng nguy hiểm nhất.

3.1.2.1. HTML dựa trên thư điện tử

3.1.2.2. Chặn tin đính kèm (attachment Blocking)

3.1.2.3. Ưu điểm

- Vượt qua sự làm rắc rối hóa HTML; - Loại được các virus đính kèm tệp tin.

3.1.2.4. Nhược điểm

- Dễ đọc; - Giới hạn ký tự trong tin nhắn; - Chặn lựa chọn hợp lý.

3.1.3. Khả năng của trình duyệt

3.1.3.1. Loại bỏ trình duyệt IE (Microsoft Internet Explorer)

Trình duyệt web của Microsoft là Internet Explorer, là trình duyệt web có sẵn phức tạp nhất. Do đó nó có một hồ sơ theo dõi rất dài việc phát hiện lỗ hổng và khai thác chúng từ xa.

3.1.3.2. Gắn kèm các công cụ chống lừa đảo giả dạng (Anti-Phishing Plug-ins)

Ngày nay, ngày càng tăng số lượng các nhà sản xuất phần mềm chuyên dụng chống lừa đảo giả dạng (phishing) cung cấp trình duyệt plug-ins. Thông thường, các plug-ins được thêm vào thanh công cụ (toolbar) của trình duyệt và cung cấp một cơ sở giám sát hoạt động. Những thanh công cụ thường được gọi là "điện thoại nhà" cho mỗi URL, xác minh những máy chủ hiện tại và lập danh sách các vụ lừa đảo giả dạng.

3.1.3.3. Ưu điểm

- Cải tiến bảo mật được thực hiện tức thì, nhanh chóng. Đồng thời chuyển dần từ một trình duyệt web phức tạp thành trình duyệt với chức năng được giảm nhẹ tức

thì. Ngoài ra còn có khả năng chống lại các lỗ hổng bảo mật phổ biến nhất và lỗ hổng trong Internet Explorer.

- Tốc độ: Trình duyệt web ít phức tạp thường truy cập và xem chất liệu dựa trên web nhanh hơn.

3.1.3.4. Nhược điểm

- Mất các chức năng được mở rộng; - Việc đưa ra các ứng dụng web phức tạp.

- Phản hồi của Plug-ins: Plug-ins thường chỉ có tác dụng đối với những công cụ đã được biết đến, được phân phối rộng rãi, và các cuộc tấn công lừa đảo.

3.1.4. Sử dụng chữ ký số trong thư điện tử

Có thể nên sử dụng các hệ thống mật mã khóa công cộng để làm chữ ký kỹ thuật số trong e-mail. Việc ký này có thể được sử dụng để xác minh tính toàn vẹn của nội dung tin nhắn - từ đó xác định xem liệu nội dung tin nhắn có bị thay đổi trong quá trình gửi hay không.

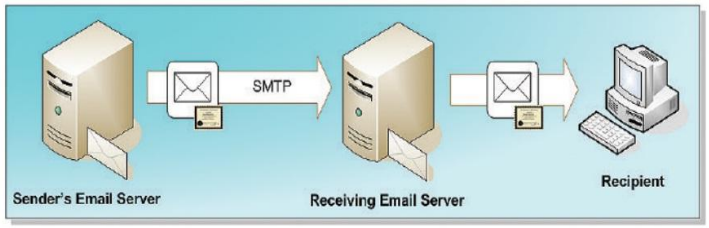


Figure 16: Digitally signed e-mail – recipient validation of authenticity

3.1.4.1. S/MIME và PGP

Hiện nay có hai phương pháp phổ biến để cung cấp chữ ký điện tử. Đó là S / MIME và PGP (bao gồm PGP / MIME và OpenPGP với tiêu chuẩn mới hơn).

3.1.4.2. Những điểm chính cho S/MIME và PGP:

• S/MIME ban đầu được phát triển bởi công ty RSA Data Security;

• PGP / MIME được dựa trên PGP, được phát triển bởi nhiều cá nhân, một số người hiện nay đã gia nhập với nhau như tập đoàn PGP.

• S/MIME, PGP / MIME, và OpenPGP MIME sử dụng để cấu trúc tin nhắn.

3.1.4.3. Ưu điểm

1) Nó đã được tích hợp vào hầu hết các tiêu chuẩn e-mail của khách hàng. Vì vậy nó có thể làm việc mà không có các yêu cầu phần cứng và yêu cầu phần mềm bổ sung.

2) Đồng nhất đường mòn kiểm toán (audit Trail). 3) Mối quan hệ tin cậy.

3.1.4.4. Nhược điểm

1) Không phải tất cả các khách hàng đều dựa trên web mail hỗ trợ S / MIME.

2) Tên miền gây hiểu lầm

3) Kiểm tra truy hồi: Người nhận có thể không kiểm tra tình trạng thu hồi chứng chỉ.

3.1.5. Cảnh giác của khách hàng

Khách hàng có thể mất một số bước để tránh trở thành nạn nhân của vụ tấn công lừa đảo trực tuyến, những bước mà liên quan đến việc kiểm tra nội dung được trình bày cho họ và đặt câu hỏi về tính xác thực của nó.

3.1.5.1. Rửa tiền (Scams Job)

3.1.5.2. Cách mà trò gian lận việc làm giả thực hiện

3.1.5.3. Ưu điểm: **về mặt giá cả:** Bằng cách luôn nhận thức được chiều hướng tấn công lừa đảo giả dạng phổ biến và sự hiểu biết làm thế nào để ứng phó lại chúng, khách hàng có thể có những hành động với mức chi phí hợp lý nhất để tự bảo vệ mình.

3.1.5.4. Nhược điểm

1) Thông tin quá tải; 2) Liên tục thay đổi chiến trường (Battlefield) gây nhầm lẫn cho khách hàng và che dấu bản chất thật của thông điệp.

3.2. PHÍA MÁY CHỦ

Ở phía máy chủ, bảo vệ chống lại lừa đảo có thể được tạo nên bởi:

3.2.1. Nhận thức của khách hàng

Các bước quan trọng trong việc giúp đỡ để đảm bảo nhận thức khách hàng và tiếp tục cảnh báo là:

• Nhắc nhở khách hàng liên tục.

• Cung cấp một phương pháp dễ dàng cho khách hàng để thông báo lừa đảo giả mạo, hoặc những email gian lận khác có thể được gửi trong tên của tổ chức.

• Cung cấp lời khuyên về cách làm thế nào để xác minh tính toàn vẹn của các trang web mà họ đang sử dụng.

• Xây dựng chính sách truyền thông của công ty và thực thi chúng.

• Để có hiệu quả, tổ chức phải đảm bảo rằng họ đang gửi một thông điệp rõ ràng, ngắn gọn và phù hợp cho khách hàng của họ.

• Phản ứng nhanh chóng và rõ ràng về các âm mưu đã được xác định là lừa đảo.

3.2.1.1. Ưu điểm

1) Chi phí thấp; 2) Yêu cầu về kỹ thuật thấp.

3.2.1.2. Nhược điểm

1) Yêu cầu tính nhất quán cao; 2) Thông tin dễ quá tải hệ thống

3.2.2. Giá trị truyền thông mang tính nội bộ

Bước này có thể được thực hiện bởi một tổ chức để giúp xác nhận thông tin liên lạc của khách hàng chính thức và cung cấp một phương tiện để xác định liệu có khả năng là các cuộc tấn công lừa đảo.

3.2.2.1. Thư điện tử cá nhân

E-mail gửi đến khách hàng nên được cá nhân hóa cho từng đối tượng người nhận. Các tổ chức phải đảm bảo rằng chúng không bị rò rỉ bất kỳ chi tiết bí mật nào của khách hàng trong thông tin liên lạc của họ.

3.2.2.2. Tham khảo thông báo trước đó (Previous Message Referral)

Có thể tham khảo một mẫu e-mail đã được gửi đến khách hàng - do đó cần thực hiện việc thiết lập sự tin tưởng trong truyền tin. Điều này có thể đạt được thông qua các phương tiện khác nhau.

3.2.2.3. Các cổng thông tin xác thực ứng dụng trang mạng (Web Application Validation Portals)

Các cổng thông tin web tồn tại để cho phép khách hàng sao chép / dán nội dung tin nhắn nhận được của họ vào một hình thức tương tác, và cho các ứng dụng để hiển thị rõ tính xác thực của thông điệp. Tương tự như vậy, Cần được cung cấp một giao diện mà trong đó khách hàng có thể sao chép hay dán các URL nghi ngờ mà họ đã nhận được. Các ứng dụng sau đó xác nhận liệu rằng đây có phải là một URL hợp pháp liên quan đến tổ chức không.

3.2.2.4. Hình ảnh hay âm thanh cá nhân trong thư điện tử

Có thể nhúng các dữ liệu hình ảnh hay âm thanh cá nhân trong một e-mail. Tài liệu này sẽ được cung cấp bởi các khách hàng trước đây, hoặc có chứa tương đương với một bí mật chia sẻ.

3.2.2.5. Ưu điểm

Hiệu quả: Quá trình đơn giản của cá nhân hoá thông tin liên lạc làm cho nó dễ dàng hơn nhiều đối với khách hàng trong việc xác định thông tin chính thức từ các email spam. Làm cho quá trình chứng thực nguồn tin nhanh hơn và hiệu quả hơn.

3.2.2.6. Nhược điểm

1) Cần tài nguyên bổ sung.

2) Nhận thức của khách hàng: Khách hàng có thể không sử dụng hoặc không nhận thức được tầm quan trọng của những hành động tự bảo vệ mang tính cá nhân.

3.2.3. Bảo mật ứng dụng trang mạng đối với khách hàng

Bảo mật ứng dụng web dựa trên cung cấp các phương pháp đầu tư mang lại nhiều lợi nhuận lớn nhất (bang for the buck) là phương pháp bảo vệ khách hàng chống lại các cuộc tấn công lừa đảo.

3.2.3.1. Xác thực nội dung

3.2.3.2. Xử lý phiên (Session handling)

3.2.3.3. Năng lực URL

3.2.3.4. Các quy trình thẩm định

3.2.3.5. Quy định ảnh (Image Regulation)

3.2.3.6. Ưu điểm

1) Tính mạnh mẽ; 2) Hiệu quả về mặt chi phí; 3) Độc lập đối với khách hàng

3.2.3.7. Nhược điểm

1) Cần các yêu cầu phát triển kỹ năng; 2) Phải được thử nghiệm; 3) Chi phí quản lý hiệu suất.

3.2.4. Xác thực dựa trên thẻ bài mạnh (Strong Token)

Khách hàng của các ứng dụng dựa trên web hợp pháp có thể sử dụng một thẻ vật lý giống như một thẻ thông minh hoặc máy tính để cung cấp một mật khẩu cho 1 lượt sử dụng hoặc mật khẩu sử dụng trong một khoảng thời gian nhất định (time-dependant).

Figure 18: Strong token-based authentication

3.2.4.1. Ưu điểm

1) Mật khẩu có sự phụ thuộc thời gian;

2) Truy cập thẻ bài (token) vật lý;

3) Tạo cảm giác tin tưởng.

4) Chống gian lận.

3.2.4.2. Nhược điểm.

1) Đào tạo người sử dụng;

2) Các chi phí cho thẻ bài (token);

3) Mất thời gian thiết lập;

4) Chi phí quản lý cao;

5) Các vấn đề bị chia nhỏ.

3.2.5. Máy chủ và những hiệp ước liên kết

Số lượng lớn các cuộc tấn công lừa đảo tận dụng sự nhầm lẫn bị gây ra bởi tổ chức sử dụng tên phức tạp với các dịch vụ lưu trữ-host và các URL không thể đọc được (chẳng hạn như các tên miền đầy đủ). Hầu hết khách hàng đều không hiểu về kỹ thuật và dễ dàng bị choáng ngợp với những thông tin dài và phức tạp được trình bày trong các URLs "theo sau các liên kết này". Bất cứ ở đâu cũng có thể xảy ra các cuộc tấn công lừa đảo này, nên các tổ chức cần phải:

• Luôn luôn sử dụng domain có cùng nguồn gốc.

• Tự động chuyển hướng các tên domain được đăng ký trong khu vực hoặc trong các khu vực khác tới các domain chính của công ty.

• Sử dụng các tên máy chủ-host mà đại diện cho tính chất ứng dụng dựa trên web.

• Luôn luôn sử dụng URL đơn giản nhất hay các máy chủ có thể lưu trữ tên.

• Sử dụng sự chuyển đổi địa chỉ và công nghệ cân bằng tải để tránh sử dụng của các máy chủ được đánh số.

• Không bao giờ giữ thông tin về phiên giao dịch trong 1 dạng URL.

3.2.5.1. Ưu điểm

1) Dễ áp dụng; 2) Xác định hữu hình; 3) Dễ dàng để giải thích

3.2.5.2. Nhược điểm

Sửa đổi ứng dụng: Một số các ứng dụng phức tạp với các tên máy chủ được mã hóa cứng có thể được yêu cầu cập nhật.

3.3. PHÍA DOANH NGHIỆP

Các bước quan trọng để chống lừa đảo bảo mật cho doanh nghiệp bao gồm:

3.3.1. Xác thực phía máy chủ gửi thư điện tử

Về bản chất, máy chủ gửi mail của người gửi được xác nhận (chẳng hạn như độ phân giải ngược của thông tin tên miền đến một địa chỉ IP cụ thể hoặc một phạm vi cụ thể) của máy chủ nhận mail. Nếu địa chỉ IP của người gửi không phải là một địa chỉ được uỷ quyền cho các miền e-mail, e-mail sẽ bị loại bỏ bằng máy chủ nhận mail.

Ngoài ra, thông qua việc sử dụng SMTP an toàn, vận chuyển e-mail có thể được thực hiện qua một liên kết SSL/TLS đã được mã hóa. Khi bộ gửi email của các máy chủ mail kết nối tới máy chủ mail người nhận, thì giấy chứng nhận được trao đổi trước khi một liên kết được mã hóa được thành lập. Việc xác thực các chứng chỉ có thể được

sử dụng để nhận diện một người gửi tin cậy. Việc "mất tích" chứng chỉ không hợp lệ hay bị thu hồi sẽ ngăn chặn một kết nối an toàn xảy ra và không cho phép cung cấp e-mail.

Nếu được yêu cầu, thì việc kiểm tra bổ sung với các máy chủ DNS có thể được sử dụng để đảm bảo rằng các máy chủ mail chỉ được ủy quyền có thể gửi e-mail trên các kết nối SMTP an toàn.

3.3.1.1. Ưu điểm

1) Cấu hình dễ dàng; 2) Phòng ngừa giấu tên; 3) Nhận dạng thư điện tử của doanh nghiệp.

3.3.1.2. Nhược điểm

1) Dễ dàng giả mạo địa chỉ bên gửi email; 3) Dịch vụ E-mail của bên thứ ba.

2) Chuyển tiếp thư điện tử (E-mail Forwarding); 4) Phân phối SMTP an toàn.

3.3.2. Thư điện tử sử dụng chữ ký số (Digitally Signed E-mail)

Các doanh nghiệp có thể cấu hình máy chủ nhận e-mail của họ để tự động xác nhận bằng chữ ký số e-mail trước khi chuyển đến người nhận. Ngoài ra, các máy chủ e-mail doanh nghiệp có thể được cấu hình để các e-mail gửi đi luôn được ký. Bằng cách làm như vậy, một giấy chứng nhận kỹ thuật số duy nhất "của công ty" có thể được sử dụng và khách hàng đã nhận được những chữ ký e-mail có thể tự tin rằng tin nhắn nhận được của họ là hợp pháp.

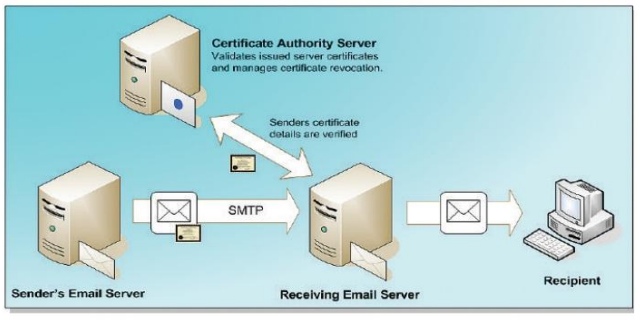


Figure 21: Digitally signed e-mail – receiving mail server validation of authenticity

3.3.3. Giám sát miền

Điều quan trọng là tổ chức một cách cẩn thận theo dõi việc đăng ký tên miền Internet liên quan đến tổ chức của họ. Các công ty nên được giám sát liên tục việc đăng ký tên miền và hệ thống tên miền cho các tên miền xâm phạm tên thương hiệu của họ, và có thể được sử dụng để tung ra các trang web giả mạo để đánh lừa khách hàng. Có hai lĩnh vực quan tâm:

3.3.3.1. Tên miền hết hạn và gia hạn mới

3.3.3.2. Đăng ký tên miền có tên tương tự nhau

3.3.4. Các dịch vụ cổng (Gateway services)

Các vành đai mạng doanh nghiệp là một nơi lý tưởng cho việc thêm các dịch vụ bảo vệ cửa ngõ mà có thể giám sát và kiểm soát cả thông tin liên lạc trong và ngoài nước. Những dịch vụ này có thể được sử dụng để xác định nội dung lừa đảo giả dạng độc hại; cho dù nó nằm trong e-mail hoặc trong các luồng truyền thông khác. Các dịch vụ cổng cấp doanh nghiệp điển hình bao gồm:

- Cổng Anti-Virus Scanning;
- Cổng Anti-Spam Filtering
- Cổng Content Filtering;
- Các dịch vụ Proxy

3.3.4.1. Ưu điểm

1) Cập nhật hiệu quả; 2) Sự độc lập ISP; 3) Chế độ bảo vệ được ưu tiên trước tiên.

3.3.4.2. Nhược điểm

1) Những hạn chế về lưu lượng: Một số dạng của lưu lượng mạng không thể bị quét.

2) Các thay đổi Firewall; 3) Yêu cầu sự bảo vệ người sử dụng chuyển vùng.

3.3.5. Các dịch vụ quản lý

Các dịch vụ quản lý trong các lĩnh vực chống thư spam và chống lừa đảo giả dạng cung cấp cải tiến rất có giá trị trong công tác bảo vệ an ninh.

3.3.5.1. Giám sát hoạt động của trang mạng

Các nhà cung cấp dịch vụ quản lý có thể triển khai dựa trên các chương trình tổng quan để theo dõi các URL và các nội dung web từ các trang web từ xa, tích cực tìm kiếm cho tất cả các trường hợp có logo, nhãn hiệu hàng hoá, hoặc nội dung web độc đáo của một tổ chức.

3.3.5.2. Ưu điểm

1) Dễ sử dụng; 2) Tầm nhìn rộng hơn; 3) Sự can thiệp kịp thời.

3.3.5.3. Nhược điểm

1) Tốn kém; 2) Quản lý xác thực lỗi

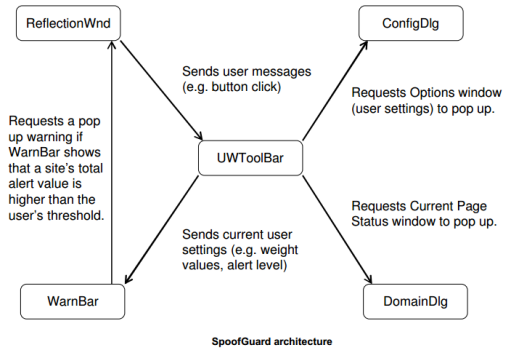
Chương 4. ỨNG DỤNG PHÒNG TRÁNH TRONG TRÌNH DUYỆT

4.1. SPOOFGUARD

Là một phần bổ sung (plug-in) tương thích với Internet Explorer.

4.1.1. Kiến trúc của SpoofGuard

Sự tương tác giữa các phân hệ chính, mô tả dưới đây, được thể hiện trong hình:



SpoofGuard architecture

Các phân hệ trên chính là các hàm được lập trình tạo nên chương trình SpoofGuard, với vai trò cụ thể sau:

4.1.2. Cài đặt

Tải phần mềm SpoofGuard về tại link: https://crypto.stanford.edu/SpoofGuard/ Chạy file cài đặt, khởi động lại trình duyệt, trong cửa sổ trình duyệt, tại thanh công cụ, nhấn chuột phải rồi chọn WarnBar Class.

4.1.3. Giao diện

Thanh công cụ SpoofGuard có 3 nút: Settings (nơi người dùng thiết lập các thông số), Status (hiển thị miền website mà bạn truy cập) và Reset (xóa mọi dữ liệu mà SpoofGuard thu thập được, nhưng không xóa History của Internet Explorer).

4.1.4. Nguyên lý hoạt động

Khi người dùng truy cập vào một trang web, SpoofGuard sẽ đưa ra 5 kiểm tra (check) trong 2 vòng (round): Domain Name Check, URL check, Email Check, Password Field check và Image check. Mức độ kiểm tra của mỗi check được thể hiện thông qua 1 con số gọi là weight do người dùng thiết lập (có thể thiết lập weight cho mỗi check để cho check này có giá trị lớn hơn check kia). Kết quả của mỗi check sẽ được cộng lại với nhau, sau đó so sánh với giá trị thiết lập weight để đưa ra kết quả có phải là phishing hay không.

4.1.5. Ưu điểm và nhược điểm

4.1.5.1. Ưu điểm

+ Giúp vá một số điểm yếu về bảo mật của phần lớn các trang web hiện tại.

+ thông tin cảnh báo của SpoofGuard giúp người dùng tự xác định được cả những mối nguy hiểm tiềm tàng (nếu có) của Website.

+ SpoofGuard có khả năng phát hiện các cuộc tấn công lừa đảo Web mà không cần bất kỳ sự hợp tác từ các trang web.

4.1.5.2. Nhược điểm

+ Chỉ áp dụng được với trình duyệt Internet Explorer (IE).

+ Kỹ thuật này không thể chống lại một số dạng giả mạo nguy hiểm. Do đó chỉ áp dụng phù hợp cho phía Client, thông thường với các chuyên gia (hay phía Server) sẽ không cần dùng đến ứng dụng này.

4.2. TRANG WEB KIỂM TRA LỪA ĐẢO GIẢ DẠNG PHISH TANK

4.2.1. Cơ bản về Phish Tank

PhishTank là một website miễn phí cho mọi người có thể kiểm tra, theo dõi và chia sẻ dữ liệu về phishing.

Truy cập vào địa chỉ http://www.phishtank.com/ để sử dụng trang web này.

4.2.2. Ưu điểm

+ Giao diện thân thiện, đơn giản, dễ sử dụng.

+ Thông tin về Phishing được cập nhật nhanh chóng.

4.2.3. Nhược điểm

+ Chỉ có khả năng phòng Phishing, không có khả năng chống Phishing.

4.3. NETCRAFT

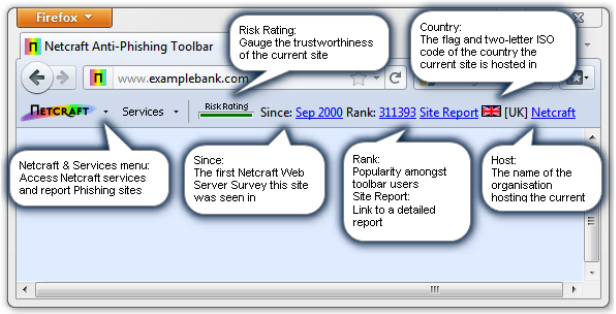
Netcraft là công ty đã khảo sát Internet từ 1995 và thu thập biến thiên của Internet trong vòng gần 20 năm qua. Đây là một công ty của Anh Quốc và có độ tin cậy rất cao. Netcraft là add-on sử dụng để giải quyết cùng vấn đề về phishing.

4.3.1. Cài đặt

Tải phần mềm Netcraft về tại link: http://toolbar.netcraft.com/install chọn trình duyệt muốn cài đặt và làm theo hướng dẫn

4.3.2. Nguyên lý hoạt động

Netcraft Toolbar cài đặt một thanh công cụ để hiển thị mức độ rủi ro (Risk rating), hạng của site (rank) và cung cấp một liên kết báo cáo (Site Report- báo cáo này cung cấp cho bạn các thông tin mà Netcraft thu thập được về site). Cũng trên công cụ này, thanh bar là một menu sổ xuống, với menu này bạn có thể báo cáo một site.



Giải thích tính năng của Netcraft trong Firefox (với Google Chrome cũng tương tự)

4.3.3. Ưu điểm và nhược điểm

4.3.3.1. Ưu điểm

+ Giao diện đơn giản, dễ hiểu và dễ sử dụng, Extension này gọn nhẹ và hầu như không có ảnh hưởng gì đến hiệu suất và vận tốc duyệt web.

+ Cung cấp chi tiết các thông tin của trang Web nhờ đó giúp người dùng có lựa chọn đúng đắn về tính toàn vẹn của trang Web.

4.3.3.2. Nhược điểm

+ Không có hiệu quả với những trang có chứa sẵn mã độc hại hay gắn kèm virus.

+ Có một số trang phishing mới không được block, có lẽ do chưa bị thông báo và chưa được cập nhật trong cơ sở dữ liệu của Netcraft.

4.4. DR.WEB ANTI-VIRUS LINK CHECKER

4.4.1. Cơ bản về Dr.Web Anti-Virus Link Checker

Dr.Web Anti-Virus Link Checker là một phần mở rộng cho trình duyệt web (hỗ trợ cả Chrome, Firefox, IE, Safari và Opera) và cả trình quản lí email Thunderbird. Dr.Web Anti-Virus Link Checker có thể phát hiện tất cả các file không an toàn trong trang web. Add-on này cũng có chức năng tự động quét tất cả các đường link trên các mạng xã hội như Facebook, Vk.com hay Google+. Dịch vụ này xuất hiện từ năm 2003 và được cập nhật theo định kỳ.

4.4.2. Ưu điểm

+ Dễ sử dụng, dung lượng chương trình nhỏ (hơn 100Mb) nên không ảnh hưởng đến hiệu năng của máy tính. Có khả năng phòng và chống Phishing cao.

4.4.3. Nhược điểm

+ Thông tin Phishing do nhà cung cấp cập nhật theo định kỳ, do đó sẽ không có tác dụng đối với các mối đe dọa mới.

4.5. TỔNG KẾT CHƯƠNG

Trong phần nghiên cứu này, tôi đã đưa ra một số phương pháp để phòng và chống Phishing. Tuy nhiên thực tế, đối mặt với Phishing có lẽ là vấn đề nan giải nhất, chúng ta không thể diệt nó, và cũng chưa có phương pháp nào để diệt nó. Trong phần này tôi đề xuất nên kết hợp nhiều phương pháp với nhau để đạt hiệu quả phòng chống Phishing tốt nhất:

Bước 1: Trước khi đăng nhập nên sử dụng công cụ Phish Tank để kiểm tra xem đây có phải trang web lừa đảo không; Bước 2: Khi đã xác nhận được đây không phải là trang web lừa đảo, sử dụng công cụ Dr.Web để kiểm tra xem có chứa virus hay phần mềm độc hại gì không; Bước 3: Sử dụng Netcraft để xác thực những thông tin về trang Web nhằm đảo bảo độ tin cậy cao hơn đối với người sử dụng. Bước 4: Trường hợp sử dụng trình duyệt là IE thì thay vì dùng Netcraft ta sử dụng công cụ SpoofGuard để xem các thông tin và các cảnh báo về khả năng Phishing của trang WEB.

KẾT LUẬN

Luận văn với đề tài "Lừa đảo qua mạng và cách phòng tránh" có các kết quả chính như sau:

1/. Tìm hiểu nghiên cứu về lừa đảo trên mạng máy tính.

2/. Thử nghiệm ứng dụng phòng tránh lừa đảo trong trình duyệt Web.

Việc ý thức được vấn nạn lừa đảo giả dạng (phishing) trên thế giới cũng như tại Việt nam là rất quan trọng. Việt Nam nổi tiếng thế giới với việc ăn cắp phần mềm có bản quyền thì không có lý gì mà "phishing" khi có điều kiện sẽ không phát triển. Để phòng và chống lại kiểu tấn công này, không có cách nào hiệu quả bằng cách giáo dục cho những người dùng máy tính những thủ đoạn lừa đảo của kẻ tấn công, lừa đảo để họ tự biết cảnh giác.

TÀI LIỆU THAM KHẢO

Tài liệu tiếng việt

[1] Nguyễn Khắc Cửu, "Bảo mật nhóm hệ thống viễn thông", đề tài luận văn thạc sỹ, Học Viện Công Nghệ Bưu Chính Viễn Thông.

[2] Nguyễn Minh Đức – Chuyên gia về Big Data, hiện đang làm việc tại Ban Công Nghệ tập đoàn FPT, bài báo "Phishing là gì? Và cách để bạn bảo vệ mình", http://securitydaily.net/phishing-la-gi-va-cach-de-ban-bao-ve-minh/ .

[3] Bài báo "Tấn công giả mạo" trên trang wikipedia, https://vi.wikipedia.org/wiki/T%E1%BA%A5n_c%C3%B4ng_gi%E1%BA%A3_m%E1%BA%A1o .

Tài liệu tiếng anh

[1] Christopher Hadnagy, "Social Engineering: The Art of Human hacking", Published by Wiley Publishing, Inc.

[2] Markus Jakobsson, "Modeling and Preventin Phishing Attacks", School of Informatics Indiana University at Bloomington Bloomington, IN 47408.

[3] Gunter Ollmann, "The Phishing Guide: Understanding and Preventing phishing attacks", Directer of Security Strategy IBM Internet Security Systems.

[4] The Anti-phishing working group, http://www.antiphishing.org