Bkav

NGHIÊN CỨU

AN NINH WIFI MIỄN PHÍ
tại các thành phố ở Việt Nam

Tháng 12 - 2014

Mục lục

Đặt vấn đề

Năm 2012, Hội An là thành phố đầu tiên ở Việt Nam đưa hệ thống mạng WiFi vào phục vụ miễn phí. Ngay sau đó, hàng loạt các thành phố, địa điểm du lịch hút khách khác trên cả nước như Hạ Long, Đà Nẵng, Huế, Hải Phòng, Đà Lạt, Tam Đảo cũng triển khai phủ sóng WiFi miễn phí, giúp người dân và du khách có thể truy cập Internet một cách thuận tiện. Hà Nội và Bắc Ninh cũng theo đuổi các dự án này nhưng còn trong quá trình triển khai.

Lợi ích thì rất dễ thấy, người dân và du khách có thể kết nối Internet một cách thuận tiện mà không phải mất thêm một khoản chi phí nào. Tuy nhiên, từ kinh nghiệm thực tế, các chuyên gia của Bkav nhận định việc sử dụng WiFi miễn phí đặt người dùng trước rất nhiều nguy cơ về an ninh an toàn thông tin. Các thành phố phủ sóng trên diện rộng, đồng nghĩa với việc lượng người dùng tăng vọt và liên tục thay đổi, các nguy cơ do đó cũng tăng cao. Trong khi đó, ý thức của người sử dụng chưa cao dù các vụ lộ lọt dữ liệu cá nhân vẫn xảy ra hằng ngày.

Từ nhận định đó, Bkav quyết định thực hiện nghiên cứu thực tế về tính an ninh khi sử dụng WiFi miễn phí tại các thành phố, đô thị du lịch của Việt Nam có cung cấp dịch vụ này. Nghiên cứu nhằm giúp người dùng hình dung được những nguy cơ họ sẽ phải đối mặt khi sử dụng mạng WiFi miễn phí, đồng thời từ đó đưa ra khuyến cáo phù hợp đến người dùng.

Phương pháp nghiên cứu

1. Thời gian, địa điểm nghiên cứu

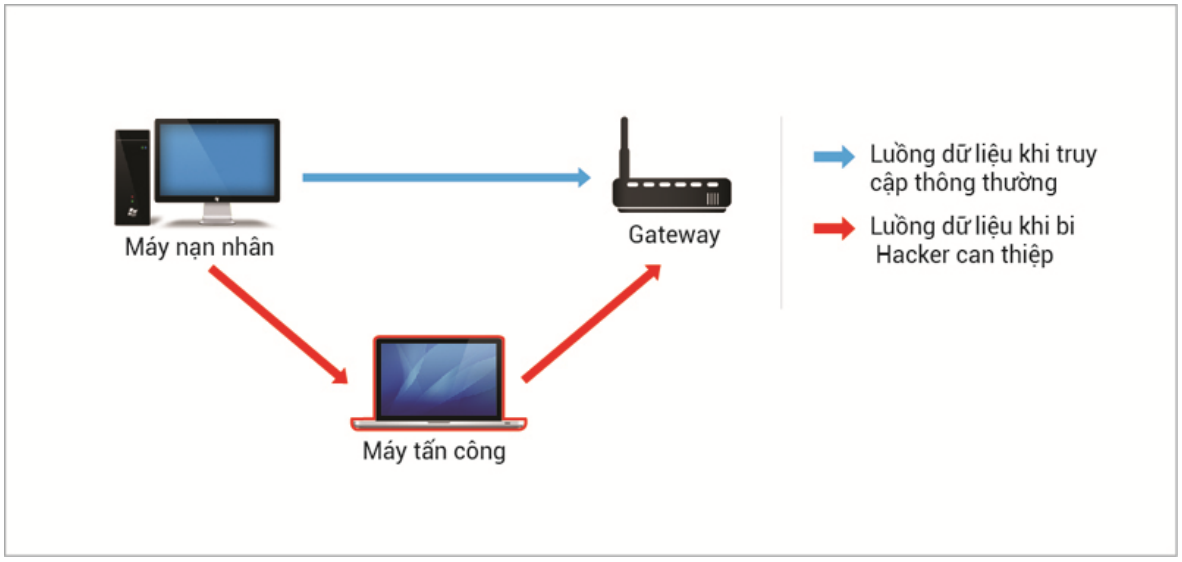
Chúng tôi quyết định thực hiện nghiên cứu tại tất cả các thành phố, khu du lịch có phủ sóng WiFi miễn phí trên cả nước. Đến trước khi Bkav bắt đầu nghiên cứu, có 7 địa phương công bố cung cấp dịch vụ này, bao gồm: Hội An, Hạ Long, Đà Nẵng, Hải Phòng, Tam Đảo, Huế, Đà Lạt. Tuy nhiên, theo thông tin thực tế chúng tôi nắm được, tại Huế và Đà Lạt WiFi miễn phí được triển khai phục vụ cho sự kiện Festival (Huế) và Tuần Văn hóa – Du lịch 2013 (Đà Lạt). Sau các sự kiện này, WiFi miễn phí không còn nữa, hoặc còn nhưng khi kết nối không truy cập được Internet. Do đó, chúng tôi quyết định tiến hành nghiên cứu ở 5 thành phố, khu du lịch còn lại là Hội An, Hạ Long, Đà Nẵng, Hải Phòng và Tam Đảo.

Nghiên cứu được tiến hành từ tháng 8 đến tháng 11 năm 2014.

2. Định hướng nghiên cứu

Theo kinh nghiệm của Bkav, 2 hình thức tấn công chủ yếu và là nguy cơ cao nhất đối với người dùng WiFi miễn phí là tấn công nghe lén thông tin Man-in-the-Middle (MitM) và tấn công lừa đảo Phishing. Bên cạnh đó, tấn công bằng hình thức phát WiFi giả mạo SSID Spoofing cũng là mối đe dọa đáng lưu ý khi người dùng kết nối Internet tại những địa điểm này. Chúng tôi quyết định đây sẽ là 3 nội dung chính trong nghiên cứu sắp thực hiện.

Về mặt kỹ thuật, hình thức tấn công MitM lợi dụng cơ chế trong giao thức ARP, từ đó giả mạo Gateway trong mạng để "nghe lén" người dùng. Trong khi đó, kỹ thuật Phishing bao gồm việc dựng một website giả mạo, tấn công DNS để điều hướng và lừa người sử dụng truy cập.



Ảnh 1: Minh họa việc tin tặc tấn công trên đường truyền

Để có thể kiểm nghiệm thực tế điều này tại các hệ thống WiFi miễn phí, chúng tôi sẽ sử dụng 2 máy tính. Máy A đóng vai trò người sử dụng, tiến hành kết nối đến mạng WiFi miễn phí và sử dụng mạng một cách bình thường. Máy B trong vai trò kẻ tấn công, cũng kết nối mạng WiFi miễn phí đó, sử dụng công cụ đã chuẩn bị sẵn để tiến hành tấn công nạn nhân (Máy A).

Các công cụ chuyên dụng được Bkav sử dụng cho máy tính tấn công bao gồm các tính năng: lợi dụng ARP Poisoning để quét mạng, nghe lén các thông tin HTTP thường; dựng mô phỏng các site HTTPS kết hợp DNS Poisoning để đánh lừa người sử dụng truy cập; phát mạng WiFi giả mạo.

3. Tiến hành nghiên cứu

Sau khi đã lên kế hoạch chi tiết, chuẩn bị kỹ càng về hạ tầng và chọn được địa điểm, thời gian, các chuyên gia của Bkav trực tiếp đi đến từng thành phố được lựa chọn để tiến hành nghiên cứu. Việc nghiên cứu thực tế bao gồm 2 bước: Kết nối vào mạng WiFi miễn phí và Thử nghiệm tấn công.

Bước 1: Kết nối vào mạng WiFi miễn phí

Tại thành phố Hải Phòng, chúng tôi lựa chọn khu vực Vườn hoa trung tâm để bắt đầu thực hiện nghiên cứu. Theo thông tin được cung cấp trên báo chí, đây là 1 trong 3 khu vực có sóng WiFi mạnh nhất tại Hải Phòng. Tuy nhiên, sau khi kết nối thành công, chúng tôi nhận thấy chất lượng sóng WiFi tại đây khá chập chờn, thường xảy ra hiện tượng mất kết nối. Khảo sát người dân, đa phần mọi người đều không biết hoặc có biết cũng không sử dụng mạng WiFi này. Tất cả các quán cafe xung quanh đều tự trang bị thiết bị phát sóng WiFi riêng và không sử dụng mạng WiFi miễn phí của thành phố.

Chúng tôi quyết định tìm đến một địa điểm khác để thực hiện khảo sát, và lần này là Trung tâm hội nghị thành phố. Chất lượng sóng WiFi tại đây tương đối ổn định, nhờ đó chúng tôi có thể thực hiện thử nghiệm theo kế hoạch.

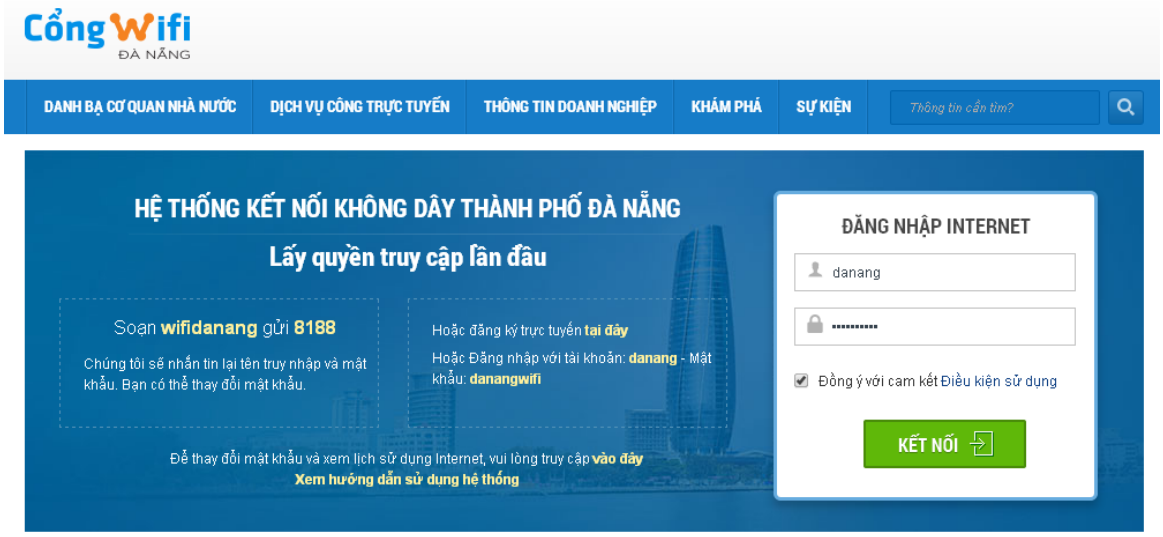
Tại Đà Nẵng, các địa điểm khảo sát có mạng WiFi tương đối ổn định bao gồm khu vực dọc bờ sông Hàn, đoạn đường Bạch Đằng, Trần Phú… Do đã có kinh nghiệm từ lần khảo sát tại Hải Phòng, quá trình khảo sát tại Đà Nẵng diễn ra tương đối thuận lợi, số lượng người sử dụng tại đây cũng nhiều hơn. Sau khi kết nối, người dùng tại Đà Nẵng được sử dụng trong khoảng giới hạn thời gian là 1 tiếng.

Ở trung tâm khu phố cổ Hội An - Quảng Nam, không có hiện tượng mất kết nối hay bị giới hạn thời gian sử dụng. Tuy nhiên, tốc độ truy cập mạng ở đây khá chậm.

Tại Hạ Long, chúng tôi thử kết nối vào WiFi miễn phí tại ba địa điểm là Trung tâm hành chính thành phố, Ngã ba Kênh Liêm và Bưu điện Hòn Gai. Theo thông tin từ các phương tiện truyền thông đại chúng, WiFi tại các địa điểm này miễn phí khi truy cập vào một số trang thông tin điện tử của tỉnh, nếu muốn vào các website khác thì người dùng phải trả phí qua thẻ cào. Tuy nhiên, tại thời điểm khảo sát, chúng tôi không thể truy cập vào WiFi miễn phí dù cột sóng trên thiết bị ở mức trung bình. Chúng tôi đã liên hệ với Bưu điện thành phố để mua thẻ cào sử dụng WiFi nhưng nhân viên tại đây cho biết không cung cấp loại thẻ cào này.

Địa điểm khảo sát tiếp theo của chúng tôi là khu du lịch Tam Đảo (Vĩnh Phúc). Tại đây, 2 WiFi miễn phí cùng tồn tại là TAMDAO_WIFI_FREE và TAMDAO_WIFI_FREE1 có tốc độ truy cập trung bình, đôi lúc chậm. Người dùng khi kết nối tới 2 mạng WiFi này không cần nhập tài khoản và mật khẩu. Việc thử nghiệm tấn công của chúng tôi diễn ra tương đối dễ dàng. Tuy nhiên, do nhà cung cấp dịch vụ áp dụng một biện pháp an ninh, việc quét mạng tìm kiếm nạn nhân có số lượng kết quả ít hơn so với khi thử nghiệm tại Hải Phòng hay Đà Nẵng.

Trừ Hạ Long, điểm cộng của các mạng WiFi miễn phí tại các thành phố khác là phía nhà cung cấp đều có hướng dẫn chi tiết để khách du lịch và người dân dễ dàng sử dụng. Thông qua các cổng thông tin điện tử tại các thành phố như HaiPhong.gov.vn, WiFi.DaNang.gov.vn, VinhPhuc.vnpt.vn… người dùng có thể kết nối vào mạng WiFi với tài khoản và mật khẩu được công bố công khai.



Ảnh 2: Dễ dàng truy cập mạng WiFi theo hướng dẫn

Ảnh 3: Thông báo từ phía nhà cung cấp khi người dùng kết nối tới WiFi miễn phí tại Tam Đảo

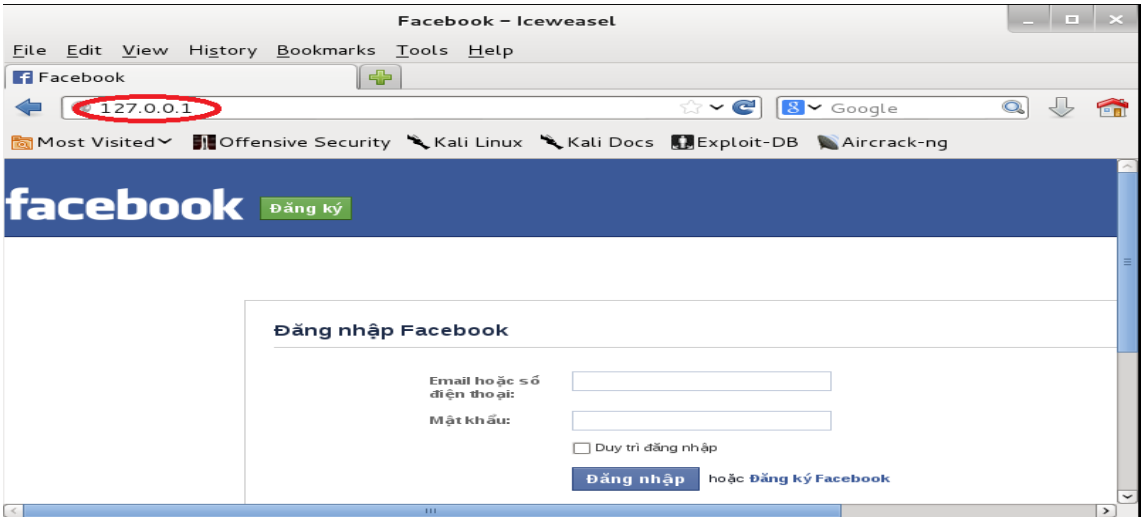
Bước 2: Thử nghiệm tấn công

Tại mỗi địa điểm, các chuyên gia của chúng tôi thử nghiệm 3 hình thức tấn công: MitM, Phishing và **SSID Spoofing**, phân tích các dữ liệu thu được và đưa ra kết luận.

Với hình thức tấn công **MitM**, máy đóng vai nạn nhân tiến hành truy cập vào các website sử dụng HTTP (thông tin trên đường truyền không được mã hóa) như HaiPhong.edu.vn, DaNang.edu.vn... Trong khi đó, máy tấn công cũng kết nối đến cùng mạng WiFi, sử dụng các công cụ đã được chuẩn bị từ trước để "nghe lén" thông tin gửi đi từ máy nạn nhân.

So với MitM, tấn công **Phishing** phức tạp hơn và chúng tôi sử dụng hình thức này cho các dịch vụ có mã hóa (HTTPS). Dịch vụ được lựa chọn ở đây là Facebook. Đây là mạng xã hội có số người dùng khổng lồ, và đặc biệt được ưa thích tại các điểm du lịch khi người dùng thường xuyên check-in để "khoe" các bức ảnh mới chụp, hay chia sẻ

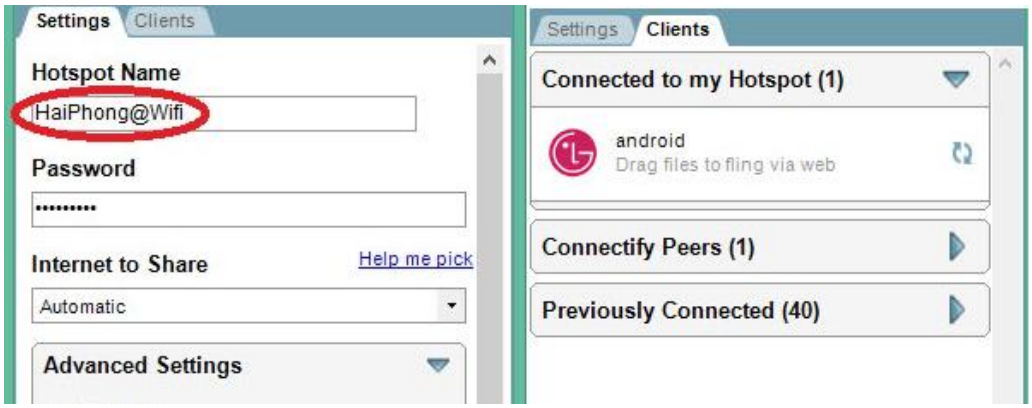
cảm xúc với bạn bè. Để tấn công, một trang Facebook giả mạo sử dụng HTTP được dựng lên trên máy hacker:



Ảnh 4: Trang Facebook giả mạo trên máy hacker

Tiếp theo bằng cách giả mạo DNS (DNS Poisoning), máy hacker điều hướng người dùng đến trang Facebook giả mạo nếu nạn nhân không chú ý đến các dấu hiệu bất thường trên trình duyệt.

Với thử nghiệm tấn công bằng WiFi giả mạo **SSID Spoofing**, chúng tôi thiết lập một thiết bị phát sóng WiFi và đặt tên trùng với tên của mạng WiFi miễn phí (HaiPhong@Wifi, DaNangWifi, HoiAnNet_MegaWifi…). Việc tiếp theo là chờ kết nối từ nạn nhân.

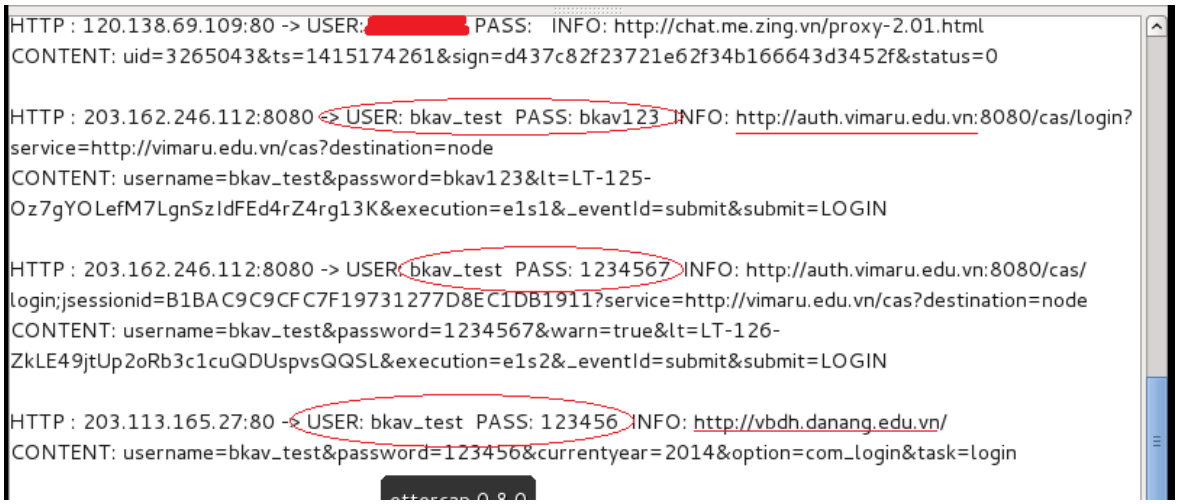


Ảnh 5: Phát WiFi giả mạo để lừa người sử dụng kết nối

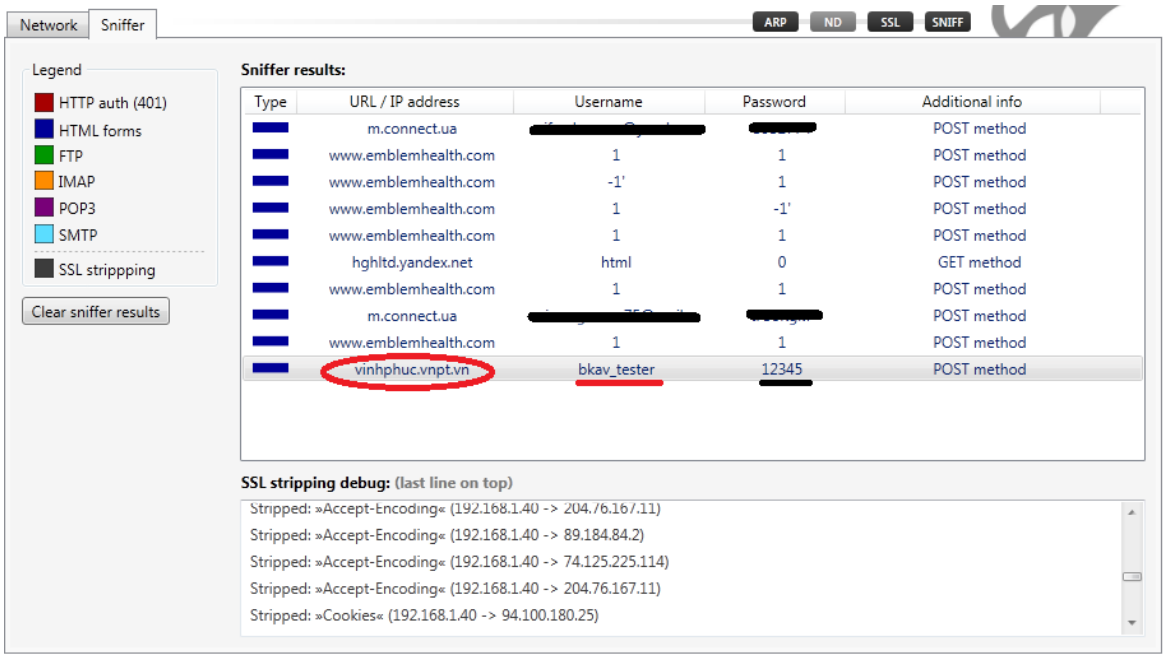
Các phát hiện chính

1. Nguy cơ tấn công MitM

Kết quả cho thấy, 100% các dữ liệu trên đường truyền của máy nạn nhân đều bị nghe lén và những dữ liệu không được mã hóa sẽ ở dạng plain-text dễ dàng đọc được.



Ảnh 6: Các thông tin HTTP bị nghe lén khi truy cập WiFi miễn phí tại Hải Phòng và Đà Nẵng



Ảnh 7: Kết quả thu được khi tiến hành tấn công tại Tam Đảo

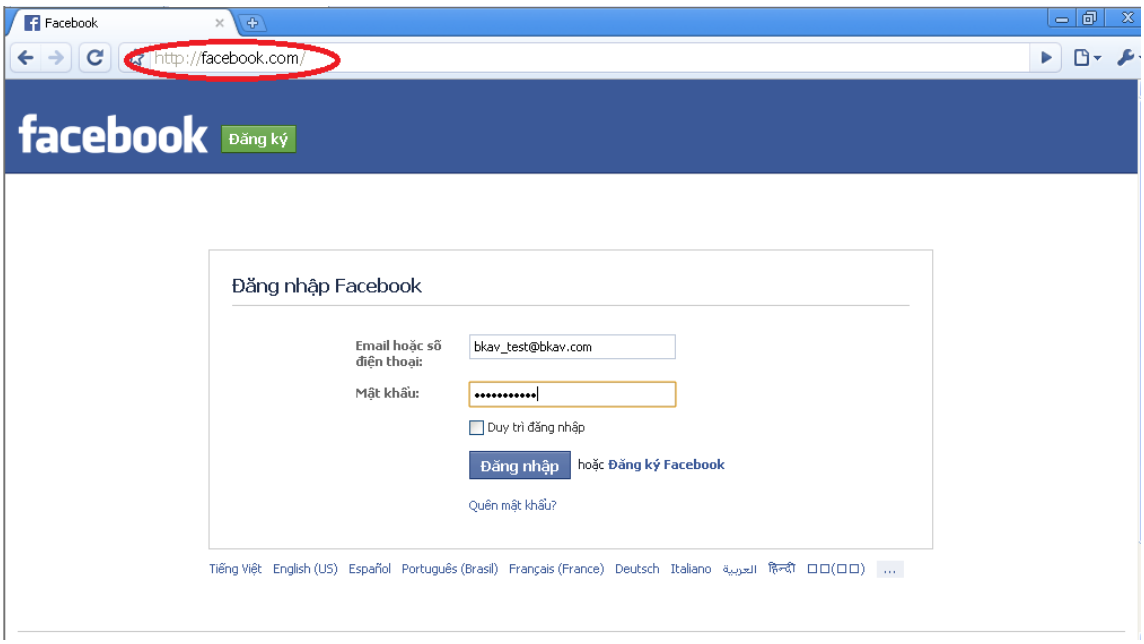
Như hình chụp lại kết quả từ công cụ quét có thể thấy, những thông tin dạng Tên đăng nhập - Mật khẩu, cũng như session, cookie, UID của nạn nhân khi truy cập vào các website sử dụng HTTP thường đã bị lộ.

Điều này là hoàn toàn dễ hiểu, bởi đây vốn là lỗ hổng thiết kế nằm trong ARP, giao thức phân giải địa chỉ, cho phép xác định địa chỉ MAC và IP của một thiết bị kết nối trong mạng. Một thiết bị muốn truy cập cần xác định được IP và MAC của Gateway. Lợi dụng điều này, máy tấn công sẽ tiến hành giả mạo địa chỉ MAC của Gateway trong mạng, từ đó nghe lén toàn bộ nội dung từ phía máy nạn nhân.

Lỗ hổng này trong giao thức ARP vốn chỉ có thể được khắc phục đối với các mạng WiFi có quy mô nhỏ, lượng người dùng không quá nhiều và quản trị có thể cấu hình nhận biết từng địa chỉ MAC cố định với từng IP. Điều này là không thể đối với mạng WiFi miễn phí có số lượng người dùng lớn và thường xuyên thay đổi.

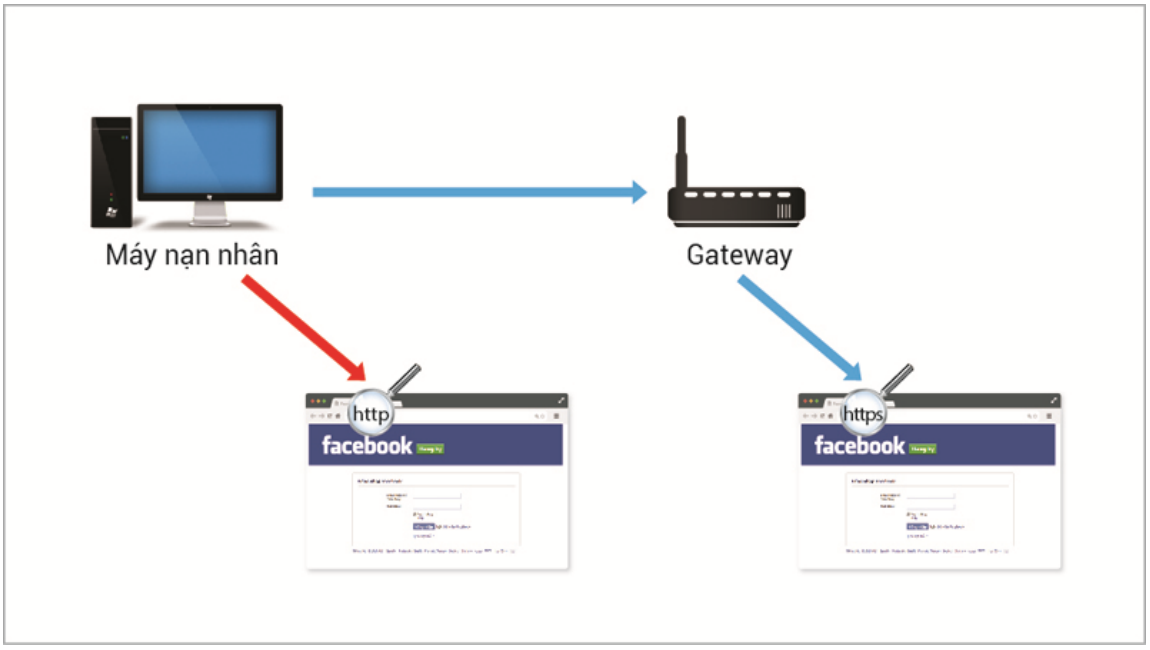
2. Nguy cơ tấn công Phishing

Từ khảo sát cho thấy, dù với các dịch vụ được mã hóa (sử dụng giao thức HTTPS) thông tin vẫn có thể bị nghe lén nếu người dùng bị tấn công bằng hình thức Phishing.



Ảnh 8: Facebook đã bị chuyển sang HTTP (thay vì HTTPS như bình thường)

Như ở ví dụ trên, chỉ cần người dùng không để ý đến thay đổi trên trình duyệt và tiếp tục click vào nút "Đăng nhập", thông tin về tài khoản và mật khẩu sẽ ngay lập tức bị gửi sang máy hacker mà hoàn toàn không được mã hóa.

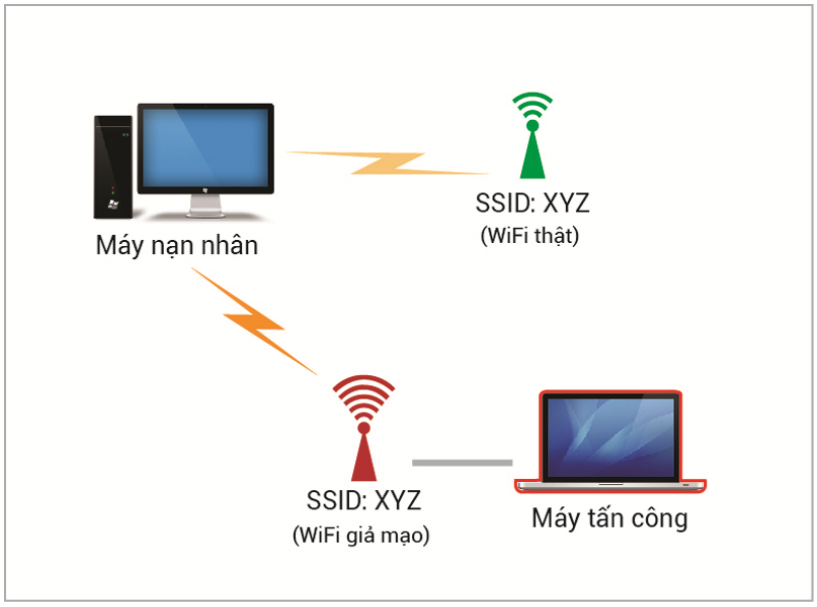


Ảnh 9: Mô hình tấn công lừa đảo Phishing

Trên thực tế, các website tài chính, kinh tế, mạng xã hội thường được truy cập hiện nay đều dễ dàng bị giả mạo thành site sử dụng HTTP. Nguy cơ do người dùng không cẩn trọng và sử dụng dịch vụ giả mạo, dẫn đến bị lộ lọt thông tin là rất cao.

3. Nguy cơ tấn công SSID Spoofing

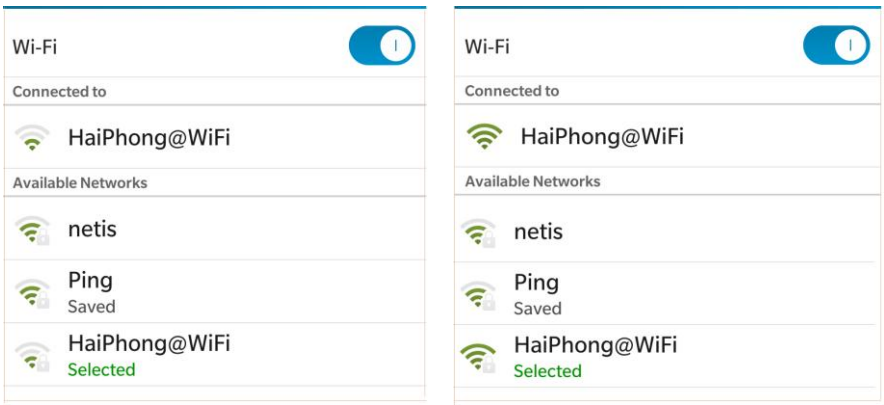
Với hình thức này, khi nạn nhân đã kết nối vào mạng WiFi giả mạo, các kỹ thuật nghe lén MitM cũng như Phishing trở nên đơn giản hơn nhiều. Trên máy đóng vai hacker, chúng tôi chỉ cần bật một số công cụ đặc biệt để đọc gói tin và phân tích kết quả thu được từ phía nạn nhân.



Ảnh 10: Mô hình tấn công giả mạo WiFi SSID Spoofing

Theo kinh nghiệm thực tế, người sử dụng mạng WiFi miễn phí rất khó có thể nhận ra đâu là mạng WiFi thật và đâu là mạng WiFi giả mạo. Có một mẹo nhỏ là người dùng nên nghi ngờ khi thấy sóng WiFi miễn phí bỗng nhiên mạnh bất ngờ. Bởi sóng WiFi miễn phí thường không được mạnh, mức sóng chỉ ở khoảng 60% đến 80%. Trong khi đó, kẻ tấn công dưới hình thức này sẽ phải tiếp cận gần nạn nhân, sóng WiFi do đó thường "đầy vạch".

So sánh giữa mạng WiFi thực tế và mạng WiFi giả mạo:



Ảnh 11: So với mạng WiFi miễn phí thật (bên trái), mạng WiFi giả mạo (bên phải) thường có "đầy" cột sóng

Kết luận và khuyến cáo

Từ khảo sát trên, chúng ta có thể thấy nguy cơ đối với người dùng mạng WiFi là thực tế và không phải là một việc gì đó xa vời. Điều đáng lo ngại là bạn dường như không thể biết được có hacker nào đang dùng chung mạng WiFi với mình hay không. Việc nghe lén, lấy cắp thông tin sẽ diễn ra âm thầm và rất khó phát hiện.

Từ thực tế nghiên cứu, Bkav đưa ra một số khuyến cáo sau:

1. Về phía nhà cung cấp dịch vụ WiFi

Về mặt an ninh, một số biện pháp hạn chế mà các mạng WiFi này đang áp dụng như giới hạn thời gian sử dụng (ở Đà nẵng) hay thay đổi IP sau một khoảng thời gian (ở Hải Phòng) như hiện nay đều không mang lại hiệu quả cao. Một số kỹ thuật dùng để chống nghe lén trên đường truyền hiện nay chỉ khả thi đối với quy mô mạng WiFi nhỏ và có người sử dụng cụ thể. Việc triển khai trên diện rộng đi kèm với các nguy cơ về an ninh, do đó nhà cung cấp dịch vụ cần đưa ra cảnh báo cho người dùng khi sử dụng mạng WiFi miễn phí của mình.

2. Về phía người sử dụng dịch vụ

Bkav khuyến cáo cho người sử dụng hiện nay khi truy cập vào các mạng WiFi miễn phí này cần một số lưu ý sau:

- Không nên thực hiện các giao dịch tài chính, ngân hàng, duyệt email… khi sử dụng WiFi miễn phí. Trong trường hợp cần thiết phải sử dụng, người dùng cần kết nối VPN để đảm bảo an toàn.
- Nếu thường xuyên sử dụng WiFi miễn phí, cần chú ý vì các thiết bị hiện nay thường có chức năng tự động kết nối, việc này rất nguy hiểm khi gặp trường hợp hacker giả mạo WiFi. Một biện pháp để phòng tránh việc này là bạn tùy

chọn "Forget network" sau mỗi lần sử dụng, hoặc thiết lập để thiết bị không tự động kết nối lại nếu chưa được sự cho phép của bạn.

- Sử dụng phần mềm diệt virus, tường lửa cá nhân để bảo vệ máy tính của mình.
- Tắt tính năng chia sẻ file trên thiết bị hoặc chỉ chia sẻ nếu đã có thiết lập quyền cho các tài khoản xác định để tránh việc vô tình lộ lọt thông tin khi kết nối vào WiFi miễn phí.

Phụ lục

(1) **Tấn công nghe lén thông tin MitM (Man-in-the-Middle):** Hình thức tấn công trong đó kẻ tấn công nằm vùng trên đường kết nối với vai trò là máy trung gian trong việc trao đổi thông tin giữa hai máy tính, hai thiết bị, hay giữa một máy tính và server, nhằm nghe trộm dữ liệu nhạy cảm, đánh cắp thông tin hoặc thay đổi luồng dữ liệu trao đổi giữa các nạn nhân.

(2) **Tấn công Phishing:** Hình thức tấn công sử dụng email, tin nhắn… giả mạo là được gửi từ một nguồn đáng tin cậy, lừa người dùng nhập các thông tin nhạy cảm như tên tài khoản, mật khẩu, thông tin thẻ tín dụng… trên một website lừa đảo.

(3) **Giao thức ARP (Address Resolution Protocol):** Giao thức phân giải địa chỉ (ARP) là giao thức ánh xạ một địa chỉ IP đến một địa chỉ vật lý của máy tính (địa chỉ MAC).

(4) **Tấn công ARP Poisoning:** Phương pháp tấn công bằng cách tác động lên luồng dữ liệu trao đổi giữa các máy tính trong mạng LAN. Khai thác thành công, kẻ tấn công có thể điều hướng trao đổi giữa các máy tính trong mạng, buộc các dữ liệu này đi qua máy tính của hacker, từ đó điều khiển, thay đổi luồng dữ liệu, hoặc thực hiện tấn công DoS.

(5) **Hệ thống tên miền DNS (Domain Name System):** Hệ thống cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền.

(6) **Tấn công DNS Poisoning (hoặc DNS Cache Poisoning):** Kỹ thuật tấn công bằng cách lừa một máy tính tin rằng thông tin phân giải tên miền nhận được là đáng tin cậy. Một khi máy tính đã bị "đầu độc", người dùng sau đó bị điều hướng đến một server giả mạo khi truy cập vào một tên miền.

(7) **UID (User Identification):** Một chuỗi ký tự được các dịch vụ sử dụng để định danh người dùng.

(8) **SSID (Service Set Identifier):** Một chuỗi ký tự được sử dụng để định danh cho một mạng WiFi.

(9) **SSID Spoofing:** Kỹ thuật giả mạo hệ thống mạng WiFi bằng cách phát sóng và đặt SSID trùng tên với mạng WiFi cần giả mạo.

(10) **Gateway:** Một điểm trong mạng, đóng vai trò kết nối đến một mạng khác.

(11) **Mạng riêng ảo (Virtual Private Network - VPN):** Một mạng dành riêng để kết nối các máy tính của các công ty, tập đoàn hay các tổ chức với nhau thông qua mạng Internet công cộng.

Về Bkav

Bkav là công ty hoạt động theo mô hình Tập đoàn công nghệ trong các lĩnh vực an ninh mạng, phần mềm, chính phủ điện tử, nhà sản xuất các thiết bị điện tử thông minh và cung cấp dịch vụ Cloud Computing. Bkav là 1 trong 10 thương hiệu Nổi tiếng nhất Việt Nam do Hội Sở hữu trí tuệ Việt Nam bình chọn, nằm trong Top 10 Dịch vụ hoàn hảo do Hội Tiêu chuẩn & Bảo vệ Người tiêu dùng Việt Nam bình chọn.

Bkav là doanh nghiệp đầu tiên của Việt Nam lọt vào Danh sách các công ty hấp dẫn (Cool Vendors) tại các thị trường mới nổi trên toàn cầu do Gartner, hãng tư vấn CNTT hàng đầu thế giới công bố. Công ty đã thành lập Bkav Singapore và Bkav USA đặt tại Thung lũng Silicon, Mountain View, bang California – Mỹ.