Bkav®

5,6 TRIỆU HỆ THỐNG MẠNG TRÊN THẾ GIỚI

đang trong tình trạng 'bỏ ngỏ'

Tháng 5/2016

Mục lục

Đặt vấn đề

Từ trước đến nay chúng ta biết trong lĩnh vực phần mềm, các công ty thường xuyên đưa ra bản vá cho các sản phẩm của họ, như Microsoft có Patch Tuesday, Google từ lâu cũng có chương trình tặng thưởng cho những phát hiện về lỗ hổng trên các phần mềm của mình… **Vậy với phần cứng thì thế nào ? Cụ thể là lỗ hổng trên các router vốn được coi là cửa ngõ kết nối Internet của hệ thống thì sao ?**

Từ năm 2014, nhiều lỗ hổng an ninh trên router được phát hiện và công bố rộng rãi. Trong số này có những lỗ hổng cho phép tin tặc dễ dàng chiếm quyền điều khiển hệ thống từ xa. Tuy nhiên, một thực tế là chưa có một bản vá toàn diện nào cho các lỗ hổng này, chưa kể đến việc cập nhật bản vá cho router khó khăn hơn nhiều so với cập nhật trên phần mềm. Do đó, nhiều router đang được sử dụng thực tế chưa chắc đã được cập nhật bản vá.

Với vai trò là công ty an ninh mạng hàng đầu Việt Nam, Bkav quyết định khảo sát các router đang được người dùng trong nước sử dụng để kịp thời đưa ra cảnh báo và hướng dẫn khắc phục. Chúng tôi cũng mua cả các router mới nhất thuộc nhiều hãng sản xuất khác nhau đang được bán trên thị trường, để chắc chắn rằng đây là những thiết bị đã được đảm bảo an ninh từ trước khi xuất xưởng. Việc thực nghiệm được tiến hành tại phòng Lab của Bkav.

Kết quả làm chúng tôi ngạc nhiên. Không chỉ rất nhiều router cũ chưa được update bản vá, mà ngay cả những router mới được chúng tôi mua về (chạy phiên bản firmware mới nhất tại thời điểm khảo sát) cũng không hề an toàn. **Đây mới chỉ là khảo sát trên một số lượng các router ở Việt Nam, vậy trên thế giới có bao nhiêu hệ thống có lỗ hổng ? Các thiết bị này đều là của nhà sản xuất đến từ Trung Quốc, trong khi hầu hết các router đang được sử dụng trên khắp thế giới cũng là từ quốc gia này, vậy tình trạng an ninh cho router trên thế giới và tại chính Trung Quốc ra sao ?** Đây là lí do khiến chúng tôi đưa ra quyết định thực hiện một nghiên cứu trên diện rộng, kiểm chứng mức độ an ninh của hơn 21 triệu router có nguy cơ tồn tại lỗ hổng trên thế giới, tìm câu trả lời cho những nghi vấn của mình.

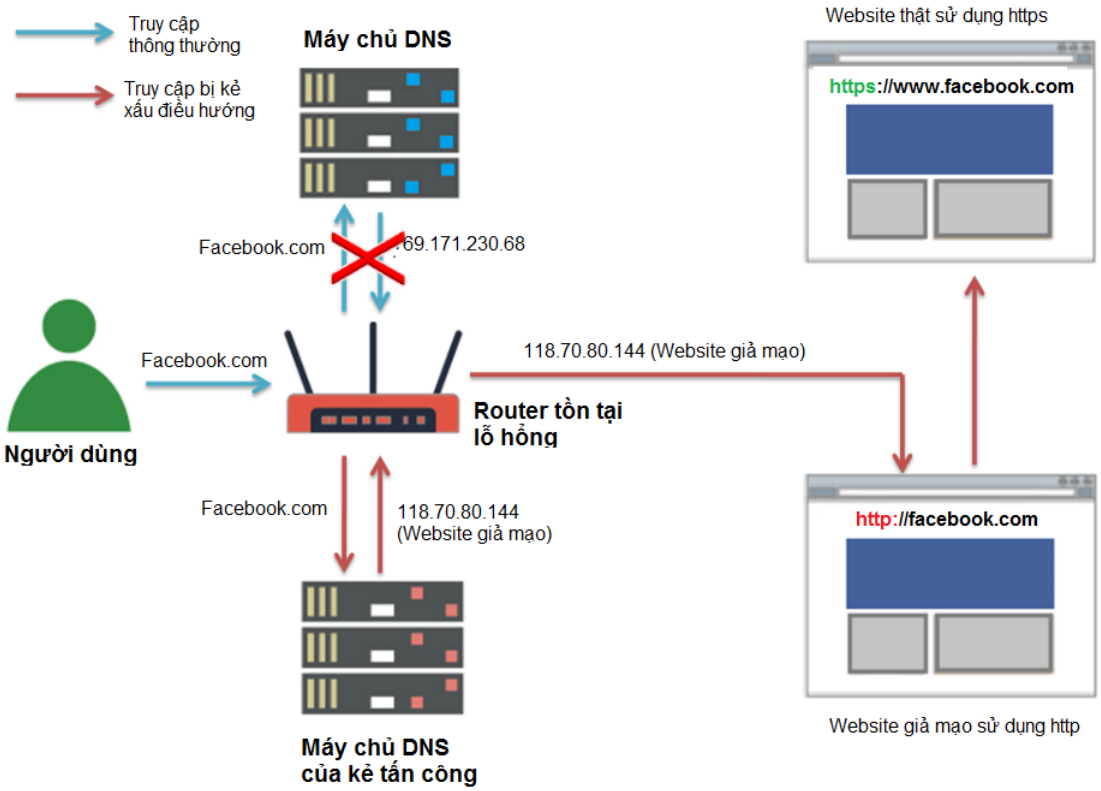
Phương pháp nghiên cứu

Nghiên cứu được thực hiện trong 2 khoảng thời gian: đợt 1 từ tháng 12/2014 đến tháng 4/2015 và đợt 2 từ tháng 12/2015 đến tháng 4/2016.

Trong mỗi đợt, việc nghiên cứu được chia thành 3 giai đoạn: Định vị phạm vi nghiên cứu; Quét trực tiếp từng IP được khảo sát trên công cụ xây dựng riêng cho dự án này; Thống kê, phân tích số liệu và xây dựng công cụ để khắc phục toàn diện.

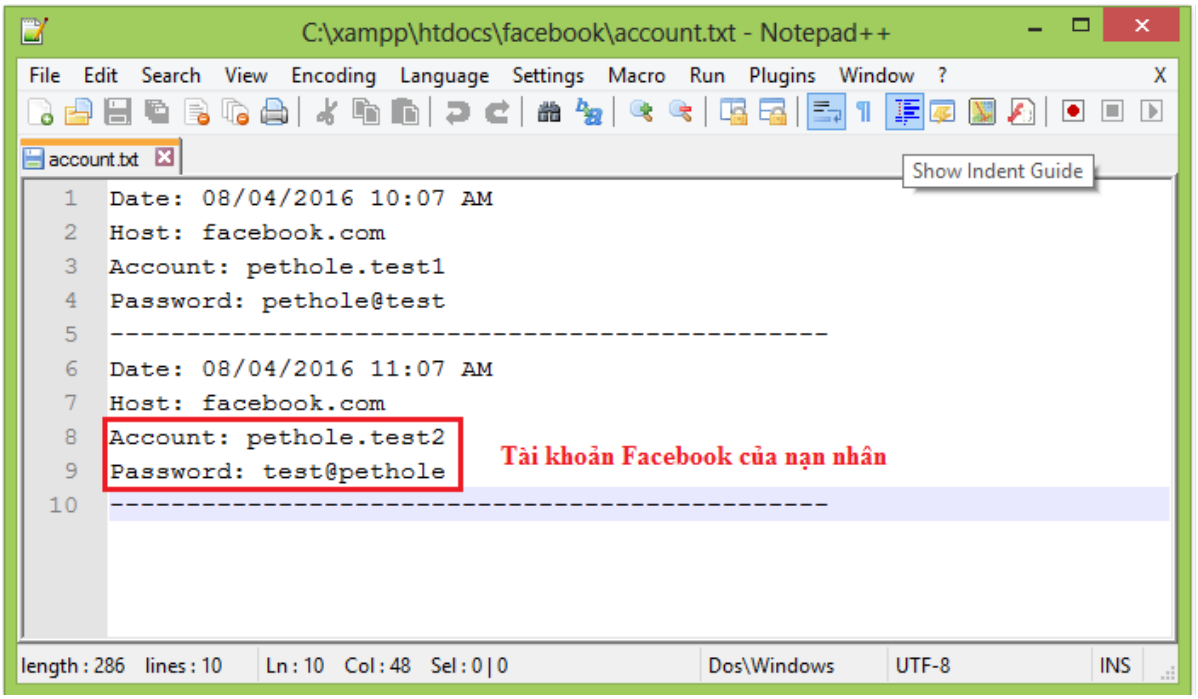
Giai đoạn 1: Định vị phạm vi nghiên cứu

Với lỗ hổng: Trong rất nhiều các lỗ hổng trên router đã được công bố, chúng tôi xác định chỉ tập trung vào ba lỗ hổng cho phép tin tặc truy cập trái phép thiết bị một cách dễ dàng. Do số lượng các router ở Việt Nam đang tồn tại các lỗ hổng này là rất lớn, Bkav dự đoán tình trạng tương tự với các router trên toàn thế giới.



Mô hình tấn công

Trong số các loại lỗ hổng trên router, lỗ hổng nguy hiểm thường gặp tồn tại trong cơ chế xác thực của trang quản trị. Lợi dụng dạng lỗ hổng này, hacker có thể vượt qua cơ chế xác thực, chiếm quyền kiểm soát router. Ngoài ra, một số loại router cho phép truy cập vào trang cấu hình DNS mà không cần đăng nhập, hacker có thể thay đổi DNS của router về server giả mạo, từ đó kiểm soát toàn bộ truy cập web của những người dùng trong mạng. Người dùng có thể bị tấn công bằng các hình thức tấn công MitM, Phishing để ăn cắp tài khoản ngân hàng, mạng xã hội, email…



Tên người dùng và mật khẩu của tài khoản Facebook thử nghiệm dưới dạng bản rõ

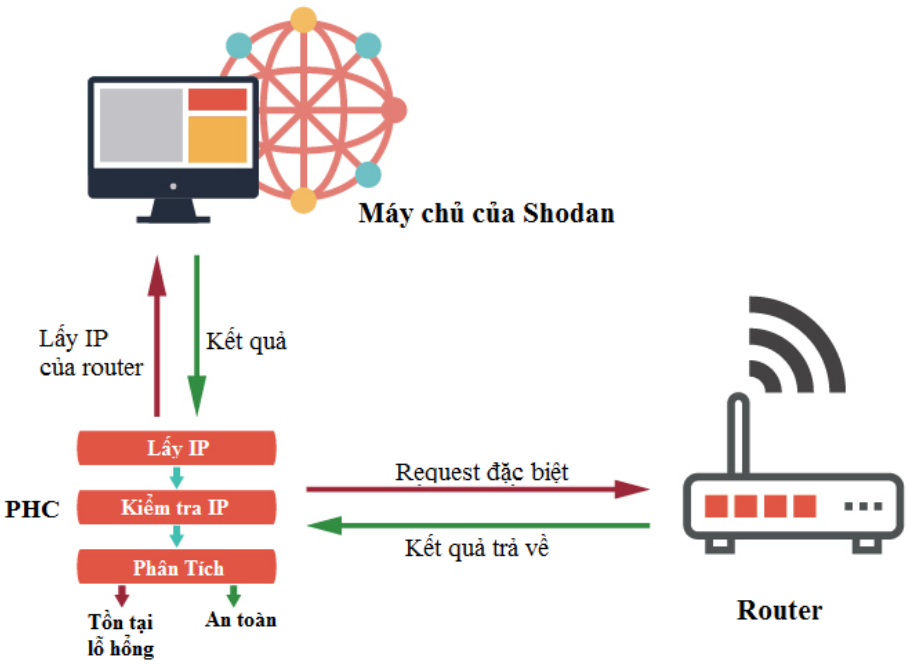
Với các Router: Để đảm bảo kết quả nghiên cứu được chính xác nhất, chúng tôi quyết định kiểm chứng sự tồn tại của lỗ hổng trên tập mẫu lớn tối đa, bao gồm tất cả các router có thể thu thập được. Chúng tôi lựa chọn sử dụng Shodan (www.shodan.io), công cụ tìm kiếm cho phép người dùng tìm kiếm với từng loại thiết bị cụ thể có kết nối Internet (router, server…). Một nghiên cứu quy mô toàn cầu được thực hiện, kết quả là **21.465.118** router đứng trước nguy cơ bị tấn công. "Đứng trước nguy cơ bị tấn công" ở đây có nghĩa là các router đó sử dụng nền tảng bị ảnh hưởng bởi 3 lỗ hổng nói

trên. *(Lưu ý: Để đảm bảo các thông tin từ nghiên cứu này không bị lợi dụng để tấn công người dùng, chúng tôi sẽ không nêu cụ thể tên các lỗ hổng. Trong phạm vi bài nghiên cứu, chúng tôi cung cấp công cụ để người dùng dễ dàng kiểm tra một router có lỗ hổng hay không, mà vẫn đảm bảo không ai biết được tên các lỗ hổng. Chúng tôi quyết định giữ bí mật tên lỗ hổng bởi các lỗi này đã được công bố từ khá lâu, chỉ cần biết tên, hacker có thể tìm kiếm trên Google và tìm ra mã khai thác).*

Đặt tên cho vấn đề: Chúng tôi đặt tên cho vấn đề này là **Pet Hole**, từ nhận định router giống như cánh cửa kết nối người dùng với Internet. Cánh cửa này đáng lẽ phải được đảm bảo an ninh nghiêm ngặt, và dù người dùng thực tế có khóa cửa nhưng lại vô tình để ngỏ những lỗ hổng để kẻ xấu có thể từ đó xâm nhập vào bên trong. Cũng giống như những Pet Door luôn luôn được mở để vật nuôi có thể ra vào dễ dàng, nhưng vô tình đó cũng chính là cơ hội để ngỏ cho kẻ xấu nếu muốn đột nhập vào bên trong.

Giai đoạn 2: Quét từng IP với công cụ được xây dựng riêng cho nghiên cứu

Để đảm bảo kiểm tra chính xác số lượng các router có lỗ hổng mà không can thiệp, vi phạm quyền riêng tư của người sử dụng, chúng tôi xây dựng riêng một hệ thống cho dự án này, **Pet Hole Checker (PHC)**. Hệ thống không lấy về mật khẩu quản trị của router, mà chỉ trả về 2 trạng thái YES và NO, với YES đồng nghĩa với việc router có lỗ hổng và có thể bị khai thác, và NO là router an toàn trước lỗ hổng.



Mô hình hoạt động của Pet Hole Checker

Giai đoạn 3: Phân tích số liệu và xây dựng công cụ khắc phục hoàn toàn lỗ hổng

Từ những dữ liệu thu thập được, chúng tôi phân tích theo nhiều hướng tiếp cận khác nhau, từ đó tìm câu trả lời cho những câu hỏi đã được đặt ra khi bắt đầu nghiên cứu này:

- Số lượng router có nguy cơ bị truy cập trái phép tại Việt Nam và trên toàn thế giới
- Các quốc gia có số lượng router tồn tại lỗ hổng nhiều nhất trên thế giới
- Tình hình lỗ hổng trên các router sử dụng tại Trung Quốc, "quê hương" của hầu hết các router trên thế giới
- Đâu là nguyên nhân, và đâu là cách khắc phục

Cũng phải nhắc lại rằng, một sự thật không thể chối cãi là mặc dù nhiều lỗ hổng an ninh nghiêm trọng đã được phát hiện, vẫn chưa có cách khắc phục nào giúp người dùng bảo vệ toàn vẹn hệ thống của mình. Chúng tôi quyết định xây dựng một công cụ nhằm đơn giản hóa công việc vốn dĩ phức tạp là kiểm tra và vá lỗ hổng router.

Các phát hiện chính

1. Hơn 5,6 triệu hệ thống mạng trên thế giới tồn tại lỗ hổng Pet Hole

5,635,024 là con số chính xác các IP của router được PHC đánh dấu là có lỗi (vulnerable). Điều này đồng nghĩa với hệ thống mạng của hơn 5 triệu hộ gia đình, thậm chí là của các cơ quan, doanh nghiệp đứng trước nguy cơ bị hacker chiếm quyền điều khiển. Để giúp người đọc hình dung rõ hơn về mức độ ảnh hưởng, hãy cùng so sánh Pet Hole với Heartbleed, lỗ hổng "nổi tiếng" nhất của năm 2014, cũng được coi là một trong những lỗ hổng nghiêm trọng nhất trong lịch sử Internet.

Tiêu chí	Pet Hole	Heartbleed
Mức độ nguy hiểm	Cao	Cao
Tỷ lệ khai thác thành công	Cao	Trung bình
Mức độ ảnh hưởng	Cao	Cao
Đối tượng có thể thực hiện	Người dùng phổ thông biết về an ninh	Chuyên gia
Khả năng vá lỗ hổng	Khó cập nhật bản vá	Tương đối dễ cập nhật bản vá

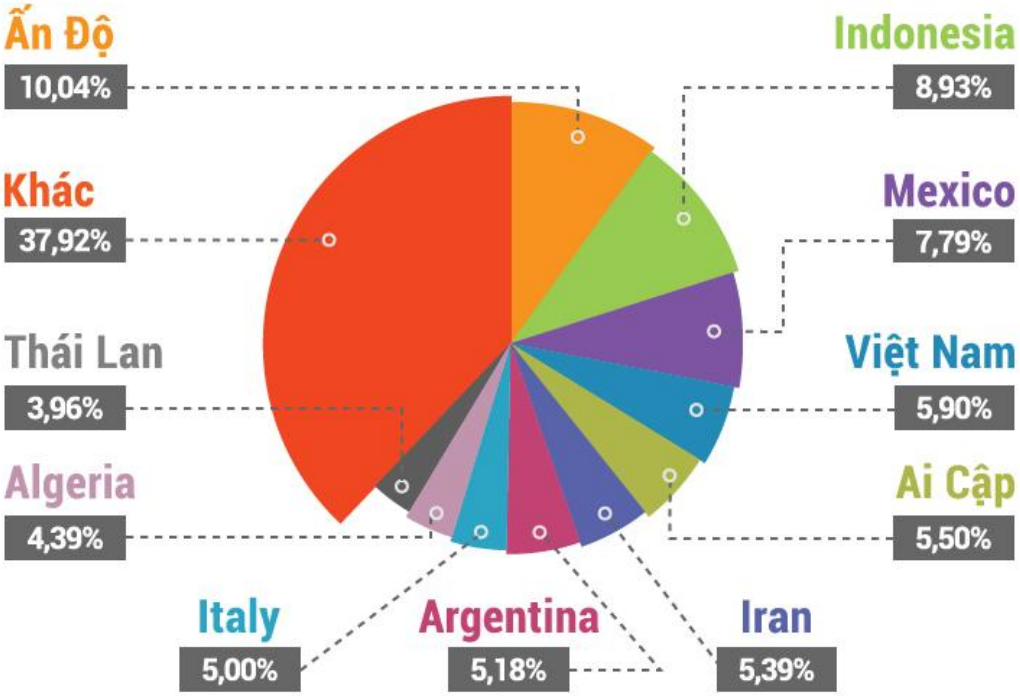
Đó là trên lý thuyết, vậy thực tế thì sao? Hãy cùng xem clip thử nghiệm Pet Hole. (Clip ghi lại quá trình thử nghiệm trên hệ thống giả lập, được kết nối Internet thông qua router có lỗ hổng được chúng tôi mua tại Việt Nam).

Vậy là đã rõ, Pet Hole thậm chí còn nguy hiểm hơn cả Heartbleed. Trong khi với Heartbleed phải là người có trình độ chuyên gia về an ninh mới có thể khai thác thành công, thì khai thác Pet Hole không cần quá nhiều kiến thức về kỹ thuật. Trong khi việc vá Heartbleed khá dễ dàng, thì vá Pet Hole lại là một công việc phức tạp. Không chỉ có vậy, clip thử nghiệm trên chứng minh rằng Pet Hole có thể dễ dàng bị khai thác trên thực tế. Để đảm bảo các nhận định trên là chính xác, chúng tôi thậm chí đã nhờ

một sinh viên IT năm 2 tham gia vào thử nghiệm. Chỉ sau một vài phút với những hướng dẫn cơ bản, cậu sinh viên đó đã có thể thay đổi cấu hình DNS của router có lỗ hổng mà không gặp bất kỳ khó khăn nào.

Tại thời điểm viết nghiên cứu này, hơn 5,6 triệu hệ thống mạng có lỗ hổng trên router, mức độ ảnh hưởng là không hề nhỏ, nếu không muốn nói là thảm họa nếu có thế lực nào đó nắm được và sử dụng khi cần thiết.

2. Ấn Độ, Indonesia, Mexico "dẫn đầu" về số lượng router có lỗ hổng

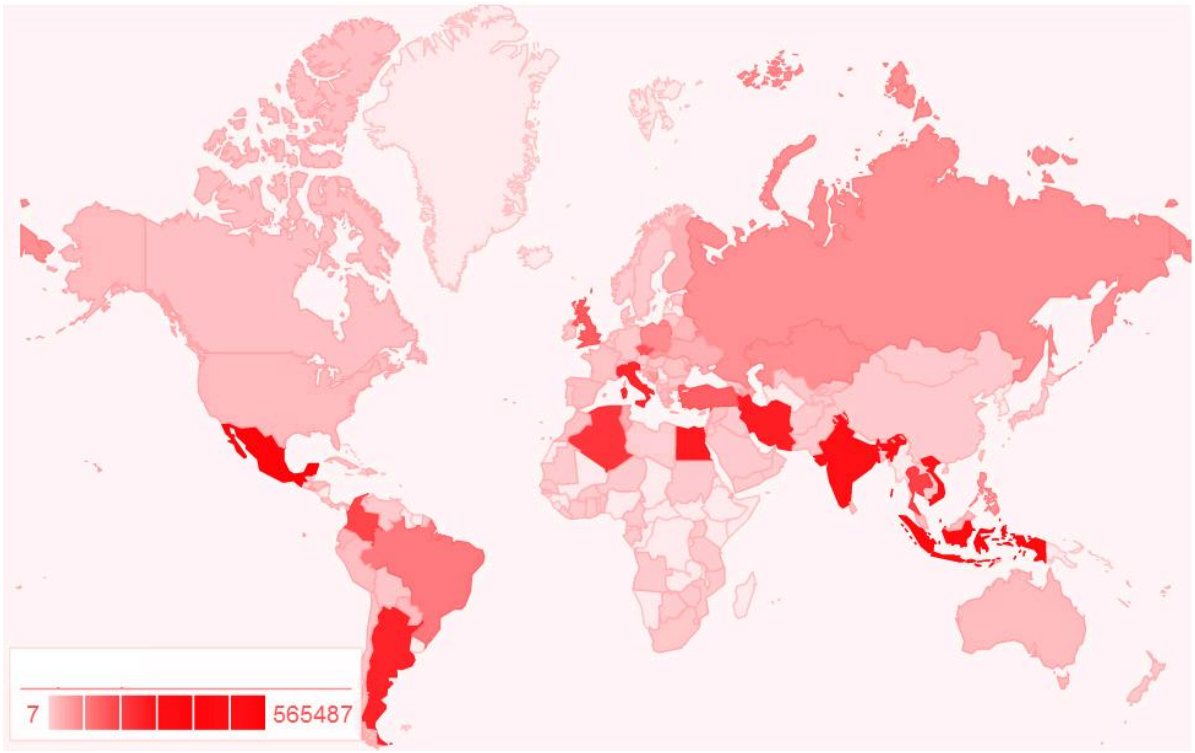


10 quốc gia "dẫn đầu" về số lượng router tồn tại lỗ hổng

Ấn Độ là quốc gia có số lượng router có lỗ hổng nhiều nhất, chiếm 10,04% (tương đương 565 nghìn). Đứng thứ 2 và thứ 3 lần lượt là Indonesia (503 nghìn) và Mexico (439 nghìn).

Điều đáng nói là trong số 10 quốc gia đứng đầu này, có đến 5 quốc gia đến từ châu Á, các châu lục còn lại đều chỉ có 2 quốc gia. Châu Á được coi là châu lục đang vươn

mình phát triển mạnh mẽ trong những thập kỷ gần đây, tuy nhiên sự phát triển nhanh đó chưa thể đi kèm với sự phát triển về cơ sở hạ tầng, trong đó có cả cơ sở hạ tầng về công nghệ. Năm quốc gia của châu Á xuất hiện trong danh sách top 10 này đều là những nước có số lượng người dùng Internet cao [1]. Châu Âu và châu Mỹ có trình độ phát triển công nghệ cao nhất. Châu Phi mặc dù cơ sở hạ tầng công nghệ chưa phát triển nhưng chỉ có 2 quốc gia nằm trong danh sách. Điều này là dễ hiểu bởi tính đến năm 2015 châu lục này mới chỉ có khoảng 20% dân số sử dụng Internet, theo ước tính của Liên minh Viễn thông Quốc tế ITU.



Bản đồ phân bố router có lỗ hổng

3. Việt Nam thuộc Top 5 quốc gia có số router bị lỗ hổng nhiều nhất

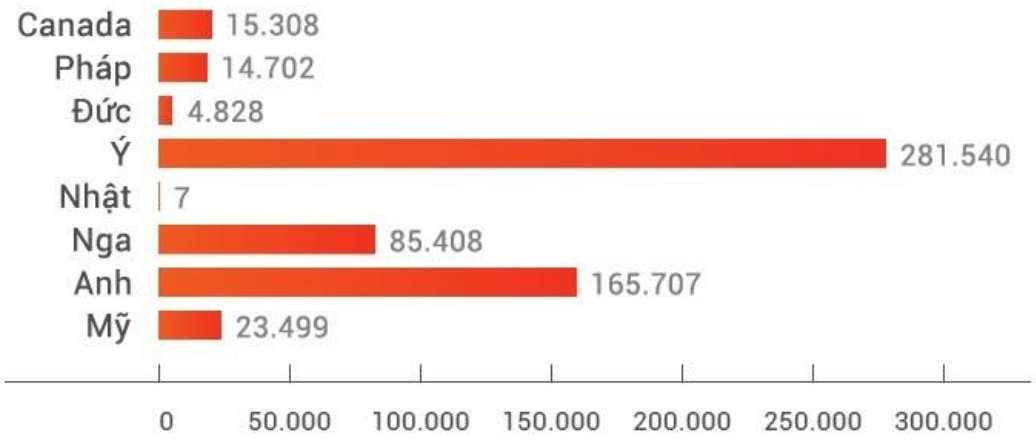
Theo kết quả nghiên cứu, Việt Nam xếp thứ 4 trong danh sách các quốc gia có số router bị lỗ hổng nhiều nhất với 332.440 thiết bị tồn tại Pet Hole.

Điều này cũng dễ hiểu, bởi Việt Nam là nước đang phát triển và nằm trong top 10 nước châu Á có tốc độ tăng trưởng người dùng Internet nhanh nhất, xếp thứ ba Đông

Nam Á, thứ 7 châu Á và thứ 18 thế giới về số người dùng Internet (Theo Sách Trắng về Công nghệ thông tin và Truyền thông Việt Nam 2014).

Router giống như cánh cửa kết nối người dùng đến Internet. Việc hơn 300 nghìn hệ thống tại Việt Nam có lỗ hổng thậm chí tiềm ẩn nguy cơ đối với an ninh quốc gia. Nếu một quốc gia có mưu đồ gián điệp đối với quốc gia khác, họ hoàn toàn có thể thực hiện việc này thông qua cửa ngõ router.

4. Hầu hết các quốc gia thuộc nhóm G8 không thuộc Top 10 quốc gia có hệ thống tồn tại lỗ hổng nhiều nhất

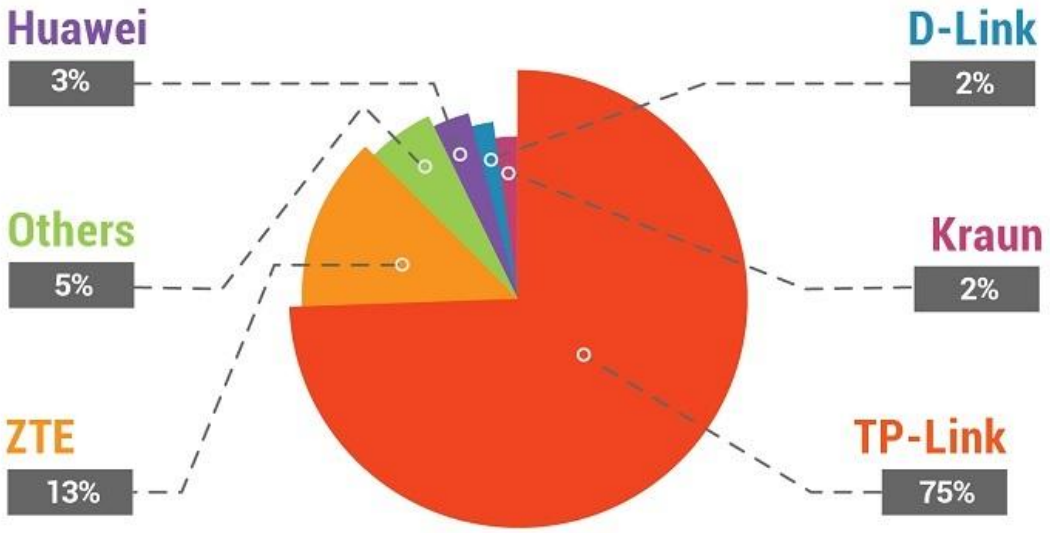


Nhìn vào biểu đồ trên có thể thấy, hầu hết các quốc gia thuộc nhóm G8 đều có số lượng không đáng kể các router có lỗ hổng. Đặc biệt, Nhật Bản chỉ có 7 router có lỗ hổng, trong khi quốc gia này thuộc top 5 thế giới về số lượng người sử dụng Internet [1].

Điều này cũng khá dễ hiểu. Đây đều là những quốc gia phát triển, nơi trình độ quản lý, bao gồm quản lý về công nghệ thông tin, tốt hơn rất nhiều so với các nước khác, tạo ra các hệ thống an ninh hơn. Bên cạnh đó, hầu hết các router sản xuất tại Trung Quốc đều thuộc phân khúc giá rẻ, được sử dụng phổ biến chủ yếu ở các quốc gia đang phát triển.

5. Hơn 90% các router có lỗ hổng được sản xuất tại Trung Quốc

Trong số các router có lỗ hổng có thể nhận dạng được tên thiết bị, chúng tôi phát hiện có tới 93% được sản xuất tại Trung Quốc, từ các hãng như TP-Link, ZTE, Huawei và D-Link. Chỉ có một số lượng rất nhỏ các nhà sản xuất khác là không đến từ quốc gia này.



Một phát hiện khác, Trung Quốc lại chỉ đứng thứ 78 xét về số lượng router có lỗ hổng Pet Hole, cụ thể là 1.281 router. Con số này khác xa so với hình dung ban đầu của chúng tôi, bởi vì Trung Quốc luôn luôn có số lượng người dùng Internet khổng lồ (đứng thứ 1 trên thế giới tại thời điểm tháng 4/2016 với hơn 720 triệu người dùng và bỏ xa quốc gia thứ 2 là Ấn Độ với hơn 460 triệu) [1]. Do đó, số lượng hệ thống có lỗ hổng đáng ra cũng không nhỏ.

Trong khi đi tìm lời giải thích, chúng tôi gặp một điều ngạc nhiên, khi hóa ra trong số 21.465.118 router được Shodan tìm ra, chỉ 83.564 router là từ Trung Quốc. Trong khi Ấn Độ, quốc gia có 462 triệu người dùng Internet – bằng 2/3 so với Trung Quốc, lại có tới 1.695.504 router tức là gấp hơn 20 lần số router xuất hiện trong cơ sở dữ liệu của Shodan. Có thể, con số này phản ánh đúng tình hình thực tế tại Trung Quốc, nơi rất ít người dùng đang sử dụng các router có nền tảng bị lỗi; hoặc Trung Quốc đã triển

khai một bức tường đặc biệt để bảo vệ các hệ thống của mình, khiến cho Shodan không thể thống kê chính xác. Dù thế nào, tỉ lệ thấp đáng ngạc nhiên tại quốc gia này cũng đáng để lưu tâm.

Kết luận và Khuyến cáo

1. Kết luận

Nghiên cứu của chúng tôi không nhằm mục đích phát hiện lỗ hổng mới, mà chỉ làm việc thống kê lại số lượng router trên thế giới vẫn tồn tại lỗ hổng nguy hiểm, cho dù thông tin về lỗ hổng đó đã được công bố rộng rãi từ trước đó rất lâu. Kết quả trên không nằm ngoài dự đoán ban đầu của chúng tôi. Số lượng các router chưa được cập nhật bản vá không hề nhỏ, và đây mới chỉ là khảo sát ba lỗ hổng nguy hiểm từ rất nhiều lỗ hổng trong thực tế. Có thể có rất nhiều những lỗ hổng khác chưa được phát hiện, thậm chí là đang được âm thầm khai thác mà người dùng không hề hay biết. Router vốn được coi như là cánh cổng kết nối mạng máy tính của bạn với thế giới Internet. Cánh cổng này không an toàn, kẻ xấu có thể dễ dàng đột nhập vào bên trong nhà bạn, hoặc có thể bí mật ngồi ở cửa theo dõi mọi hoạt động của bạn.

Vậy đâu là nguyên nhân khiến người dùng lơ là an ninh cho cửa ngõ này ?

Nguyên nhân thứ nhất rất dễ thấy, đó là việc cập nhật bản vá cho các router không hề đơn giản như khi cập nhật cho phần mềm. Nếu với phần mềm, người dùng chỉ cần làm theo hướng dẫn thường là rất đơn giản của nhà sản xuất, hoặc đôi khi là hệ thống sẽ tự động thực hiện, thì với router để lỗ hổng được cập nhật cần sự can thiệp trực tiếp từ phía người dùng. Thế nhưng, dù cho có hướng dẫn chi tiết thì không phải ai cũng có đủ kiến thức về mạng máy tính để làm theo những hướng dẫn này. Do đó, với các router sử dụng tại các hộ gia đình, khả năng người dùng bỏ ngỏ, không quan tâm dù được cảnh báo là rất cao. Với doanh nghiệp, nơi có thể có bộ phận IT riêng, việc cập nhật được coi là sẽ dễ dàng hơn. Vấn đề khi đó lại chủ yếu nằm ở chính ý thức của bộ phận IT này. Với các mạng cơ quan, doanh nghiệp, một router có thể cung cấp kết nối cho hàng chục, thậm chí hằng trăm máy tính. Do đó, chỉ cần một cơ quan, doanh nghiệp lơ là, mức độ ảnh hưởng khi router có lỗ hổng là không hề nhỏ.

Một nguyên nhân nữa không thể không nghĩ đến, đó chính là nguyên nhân đến từ chính nhà sản xuất router. Các lỗ hổng được nhắc đến trong bài nghiên cứu được công bố rộng rãi từ giữa năm 2014. Tuy nhiên, tận 2 năm sau, khi chúng tôi thực hiện nghiên cứu này thì rất nhiều những model router mới nhất bán trên thị trường vẫn chưa được cập nhật bản vá. Phải chăng, nhà cung cấp cố tình để ngỏ cửa ngõ để khi cần thì có thể can thiệp lấy thông tin, làm tê liệt hệ thống, hoặc thực hiện rất nhiều những hành động không minh bạch khác ?

An ninh từ các thiết bị Trung Quốc

Một thông tin mà ai cũng biết, đó là hầu hết các router hiện nay đều là của các nhà sản xuất Trung Quốc, hoặc của các nhà cung cấp khác nhưng được sản xuất tại quốc gia này. Trong khi đó, vấn đề an ninh trên các thiết bị của Trung Quốc từ lâu cũng đã là một dấu hỏi lớn với nhiều quốc gia. Theo kết quả của nghiên cứu này, hơn 90% các router có lỗ hổng được sản xuất tại Trung Quốc. Lý do cho vấn đề có thể nằm ở chỗ các thiết bị này không phải là thiết bị cao cấp, khiến cho chúng ít an ninh hơn; dù thế, chúng ta cũng không thể không để ý đến an ninh trên các thiết bị đến từ quốc gia này.

An ninh quốc gia bị đe dọa thế nào ?

Phải nhắc lại một lần nữa, router là cửa ngõ ra vào của mạng, kiểm soát được router là kiểm soát được toàn bộ mạng. Hơn 5,6 triệu thiết bị có lỗ hổng Pet Hole là con số không hề nhỏ. Như chúng tôi đã phân tích ở trên, để tấn công thành công lỗ hổng này không khó, hacker nghiệp dư cũng có thể khai thác thành công để chặn thông tin trao đổi của người dùng, chuyển hướng truy cập DNS để điều hướng đến website mà chúng mong muốn… Nhưng nếu mở rộng ra, nếu một quốc gia có mưu đồ theo dõi quốc gia khác, họ hoàn toàn có thể thực hiện qua cửa ngõ router này.

2. Hướng dẫn kiểm tra và khắc phục

Bkav đã phát triển công cụ để người dùng có thể kiểm tra sự tồn tại của Pet Hole trên router của mình. Người dùng chỉ cần truy cập *PetHole.net*, click vào nút "Kiểm tra Pet Hole", các thông tin liên quan đến router của bạn sẽ được hiển thị phía bên dưới. Nếu router có lỗ hổng, sẽ có hướng dẫn để người dùng có thể khắc phục vấn đề.

Tuy nhiên, tốt nhất người dùng nên cập nhật phiên bản firmware mới nhất cho router của mình. Hướng dẫn từng bước cho quá trình này cũng được cung cấp tại *PetHole.net*.

Người dùng cũng có thể xem hướng dẫn chi tiết có tại Phụ lục 2 phía dưới.

Sau khi tất cả các bước hướng dẫn đã được hoàn thành, kiểm tra router của bạn lần nữa với công cụ của chúng tôi. Nếu vẫn còn lỗ hổng, cách tốt nhất bạn có thể làm là mua một router mới.

Về Bkav

Bkav là Tập đoàn công nghệ hoạt động 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 một 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. Tập đoàn đã thành lập Bkav Singapore và Bkav USA đặt tại Thung lũng Silicon, Mountain View, bang California – Mỹ.

Phụ lục

Phụ lục 1: Danh sách các router được khảo sát trực tiếp

Nhà sản xuất	Mẫu	Thông tin
TP-Link	TD-8840t	Thời gian sản xuất: 2014 Phiên bản firmware: 17/09/15 (mới nhất tại thời điểm khảo sát)
	TD-W8951ND	Thời gian sản xuất: 2014 Phiên bản firmware: 13/01/16 (mới nhất tại thời điểm khảo sát)
	TD-8817	Thời gian sản xuất: 2014 Phiên bản firmware: 12/01/16 (mới nhất tại thời điểm khảo sát)
	TL-WR340G	Thời gian sản xuất: 2014 Phiên bản firmware: 15/07/11 (mới nhất tại thời điểm khảo sát)
	TL-WA701N	Thời gian sản xuất: 2014 Phiên bản firmware: 24/03/14 (mới nhất tại thời điểm khảo sát)
	TD-W8901	Thời gian sản xuất: 2014 Phiên bản firmware: 18/08/15 (mới nhất tại thời điểm khảo sát)
Netis	WF-2420	Thời gian sản xuất: 2014 Phiên bản firmware: 1/9/2014 (mới nhất tại thời điểm khảo sát)
D-Link	DIR-615	Thời gian sản xuất: 2014 Phiên bản firmware: 19.00 (mới nhất tại thời điểm khảo sát)
	DSL-2640B	Thời gian sản xuất: 2014 Phiên bản firmware: SEA_1.0 (mới nhất tại thời điểm khảo sát)
Tenda	A5s	Thời gian sản xuất: 2014 Phiên bản firmware: 2/5/2013 (mới nhất tại thời điểm khảo sát)

Phụ lục 2: Hướng dẫn nâng cấp firmware và tắt chức năng truy cập từ xa qua Internet

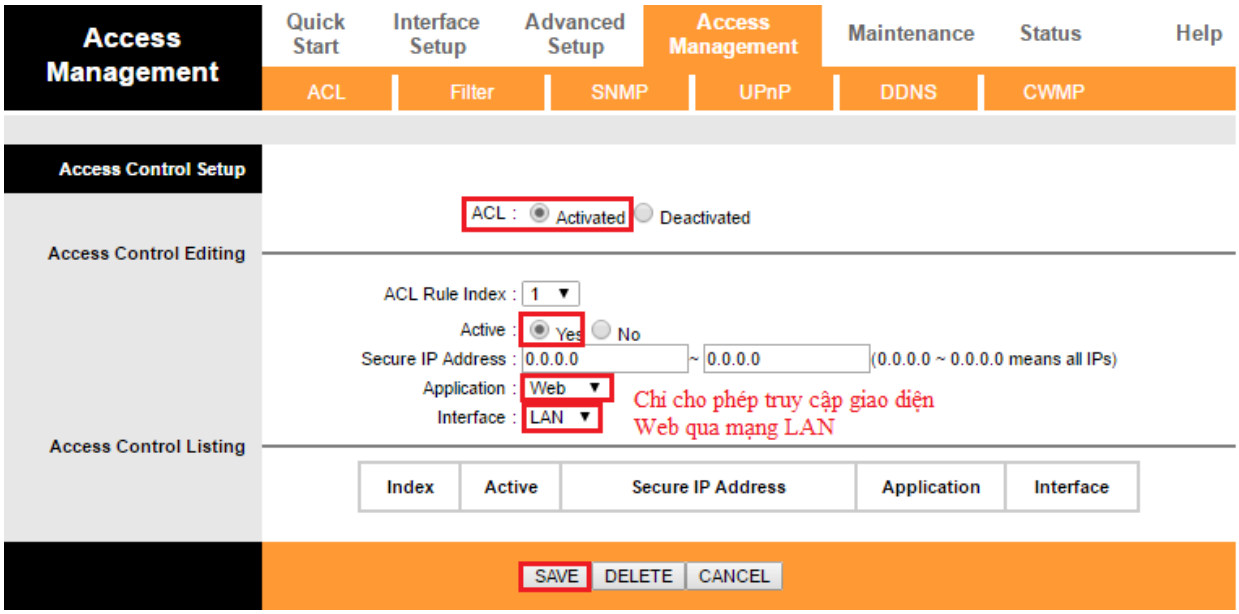
– Để nâng cấp firmware lên phiên bản mới:

  - Download firmware phiên bản cao nhất từ website của nhà cung cấp. (Không sử dụng firmware không rõ nguồn gốc, vì có thể firmware đã được chỉnh sửa để theo dõi người dùng, hoặc có thể làm hỏng thiết bị)
  - Đăng nhập vào trang quản trị thông qua địa chỉ gateway từ trình duyệt trên máy tính trong mạng. (Ví dụ địa chỉ mặc định 192.168.1.1)
  - Truy cập vào chức năng nâng cấp firmware. (Maintenance hoặc Management => Firmware)
  - Chọn "Choose file" hoặc "Browse" => chọn firmware vừa tải về
  - Chọn "Upgrade" và đợi router khởi động lại

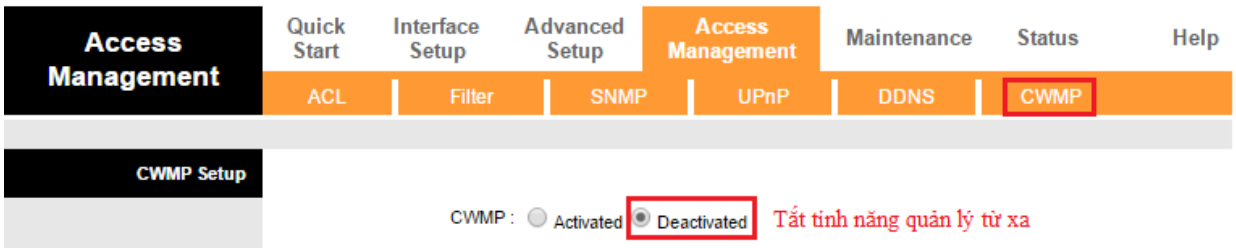
– Tắt chức năng truy cập từ xa qua Internet

Ví dụ với một loại router được dùng phổ biến tại Việt Nam là TP-Link:

  - Đăng nhập vào trang quản trị thông qua địa chỉ gateway từ một máy tính trong mạng. (Ví dụ địa chỉ mặc định 192.168.1.1)
  - Truy cập vào chức năng cài đặt kiểm soát các truy cập. (Access Management => ACL)
  - Kích hoạt ACL, tùy chọn truy cập giao diện web thông qua mạng LAN, nhấn "Save":



- Truy cập vào chức năng quản lý từ xa (Access Management => CWMP), chọn "Deactivated" và "Save":



Như vậy router của bạn đã an toàn trước kẻ xấu muốn tấn công thiết bị qua Internet.

Phụ lục 3: Số lượng các hệ thống có lỗ hổng theo quốc gia

STT	Quốc Gia	Số router có lỗ hổng
1	Ấn Độ	565.487
2	Indonesia	503.228
3	Mexico	439.176
4	Việt Nam	332.440
5	Ai Cập	310.375
6	Iran	303.928
7	Argentina	291.642
8	Italy	281.540
9	Algeria	247.501
10	Thái Lan	223.403
11	Colombia	211.082
12	Cộng hòa Séc	182.763
13	Vương quốc Anh	165.707
14	Thổ Nhĩ Kỳ	164.591
15	Brazil	124.824
16	Ba Lan	91.736
17	Kazakhstan	87.695
18	Liên bang Nga	85.408
19	Philippines	80.667
20	Bosnia và Herzegovina	72.059
21	Slovakia	62.526
22	Azerbaijan	49.381
23	Tunisia	46.104
24	Palestine	43.866
25	Ukraine	43.018
26	Phần Lan	37.385
27	El Salvador	30.704
28	Ecuador	30.617
29	Belarus	29.806
30	Mỹ	23.499
31	Úc	22.513
32	Paraguay	21.780
33	Hy Lạp	19.899
34	Malaysia	19.744
35	Peru	19.604
36	Moldova	18.651
37	Tây Ban Nha	16.925
38	Croatia	15.774

39	Canada	15.308
40	Armenia	15.013
41	Pháp	14.702
42	Romania	14.535
43	Morocco	14.432
44	Kyrgyzstan	14.390
45	Honduras	10.743
46	Cộng hòa Ả Rập Syria	10.163
47	Chile	9.836
48	Bolivia	9.496
49	Cộng hòa Dominica	9.338
50	Hungary	7.469
51	Sri Lanka	7.122
52	Thụy Sĩ	6.998
53	Albania	6.233
54	Panama	5.605
55	Israel	5.270
56	Nam Phi	5.237
57	Cuba	5.208
58	Đức	4.828
59	Uzbekistan	4.636
60	New Zealand	4.450
61	Lebanon	3.916
62	Bulgaria	3.567
63	Pakistan	3.177
64	Venezuela	3.159
65	Sudan	2.898
66	Mozambique	2.850
67	Yemen	2.800
68	New Caledonia	2.715
69	Thụy Điển	2.579
70	Ireland	2.409
71	Cam-pu-chia	1.918
72	Ghana	1.914
73	Ireland	1.833
74	Cộng hòa Macedonia	1.766
75	Hà Lan	1.540
76	Georgia	1.386
77	Cộng hòa Tanzania	1.313
78	Trung Quốc	1.281
79	Mauritania	1.198
80	Lào	1.096

81	Bồ Đào Nha	1.054
82	Bỉ	906
83	Liechtenstein	824
84	Niger	772
85	Benin	724
86	Lithuania	681
87	Afghanistan	660
88	Đan Mạnh	654
89	Các tiểu vương quốc Ả rập thống nhất	614
90	Bờ biển ngà	596
91	Bahrain	502
92	Kuwait	463
93	San Marino	461
94	Na Uy	447
95	Bangladesh	445
96	Senegal	434
97	Singapore	399
98	Áo	391
99	Cyprus	361
100	Togo	310
101	Maldives	307
102	Botswana	302
103	Cameroon	291
104	Saudi Arabia	280
105	Mauritius	248
106	Oman	245
107	Luxembourg	241
108	Brunei	238
109	Fiji	237
110	Tajikistan	189
111	Bermuda	182
112	Guadeloupe	165
113	Gabon	120
114	Costa Rica	113
115	Burkina Faso	107
116	Martinique	100
117	Uganda	100
118	Mông Cổ	100
119	Barbados	92
120	Réunion	92
121	Djibouti	85
122	Bhutan	78

123	Guatemala	69
124	Zimbabwe	63
125	Malta	59
126	Gibraltar	59
127	Angola	52
128	French Guiana	50
129	Hong Kong	50
130	Vanuatu	33
131	Faroe Islands	26
132	Đài Loan	26
133	Comoros	20
134	Estonia	20
135	Åland Islands	13
136	Iraq	13
137	French Polynesia	13
138	Jordan	7
139	Libyan Arab Jamahiriya	7
140	Đông Ti-mor	7
141	Saint Kitts và Nevis	7
142	Lesotho	7
143	Nhật Bản	7

Tham khảo

[1] Dữ liệu người dùng Internet được tham khảo từ http://www.internetlivestats.com/internet-users-by-country/, với số người dùng được tính dựa trên tỷ lệ thâm nhập (Liên minh Viễn thông Quốc Tế ITU) và dữ liệu dân số thế giới của Cục Điều tra dân số Hoa Kỳ.

[2] Sách *"Thế giới năm 2015, Thực tại và Số liệu ICT" (**The world in 2015, ICT Facts and Figures**)* của ITU http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

[3] Thông tin về lỗ hổng Heartbleed http://heartbleed.com/