



# RESEARCH

**1.4 MILLIONS  
OF ROUTERS WORLDWIDE**

**Vulnerable to Pet Hole**

April 2015

## Table of contents

<b>Problem Statement .....</b>	<b>2</b>
<b>Methodology .....</b>	<b>3</b>
Phase 1: Identifying scope of the research .....	3
Phase 2: Scanning every IP on our tool built for this project .....	5
Phase 3: Analyzing data and building tool to thoroughly fix the issue.....	6
<b>Key Findings .....</b>	<b>7</b>
1. More than 1.4 millions of networks worldwide vulnerable to Pet Hole.....	7
2. Indonesia, Egypt, Italy lead in number of vulnerable routers.....	8
3. Most members of G8+5 not appear in top 10 .....	9
4. More than 90% of vulnerable routers homed in China.....	10
5. China produces most but little routers in this country be vulnerable .....	10
<b>Conclusions and Recommendations .....</b>	<b>12</b>
1. Conclusions .....	12
2. Fixing the hole .....	13
<b>About Bkav.....</b>	<b>14</b>
<b>Appendixes .....</b>	<b>15</b>
Appendix 1: Routers experimented in Bkav's Lab .....	15
Appendix 2: Instructions to upgrade firmware & disable access from Internet .....	16
Appendix 3: Vulnerable routers by country.....	18
<b>References.....</b>	<b>23</b>

## **Problem Statement**

Software vulnerabilities have been long an important issue of Internet security. Microsoft has monthly Patch Tuesday with several patches for its software products. Google has long run a rewards program for security researchers who discover vulnerabilities in its software. **What about in network devices, specifically flaws in routers which are considered gateway connecting users to the Internet?**

Security flaws in routers seem to have got great concerns recently when many are discovered and published widely. Many of them, rated critical, allow attackers to remotely take control of systems. However, no thorough fix has been made available, not to mention updating patches for routers is inherently much harder than updating software. Several users' routers might have not been patched at all.

Being the leading Internet security firm in Vietnam, Bkav decided to carry out an experiment on routers used by local users to produce timely warning. We bought the newest modems from different manufacturers as well to make sure they are secured before reaching users. The actual experiment on modems was carried out in our Lab.

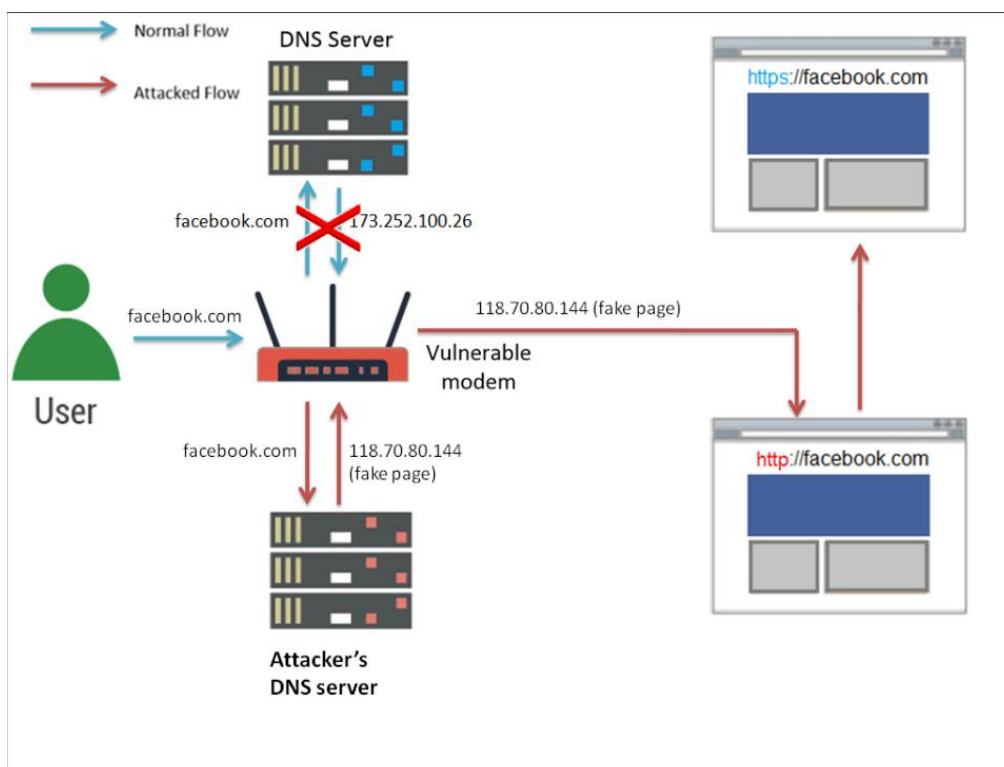
The result surprised us. Not only routers which are currently in use left unpatched, but also new ones (with the latest firmware version) not safe at all. **The experiment was carried out among a certain number of routers in Vietnam, then how many systems in the world are vulnerable? The experimented devices are all by Chinese manufacturers, while most routers in the world are from this nation, then how secured are routers in China? How to thoroughly and simply fix the issue?** This inspired Bkav to conduct a widened research to examine security of more than 10 million routers in the world.

## Methodology

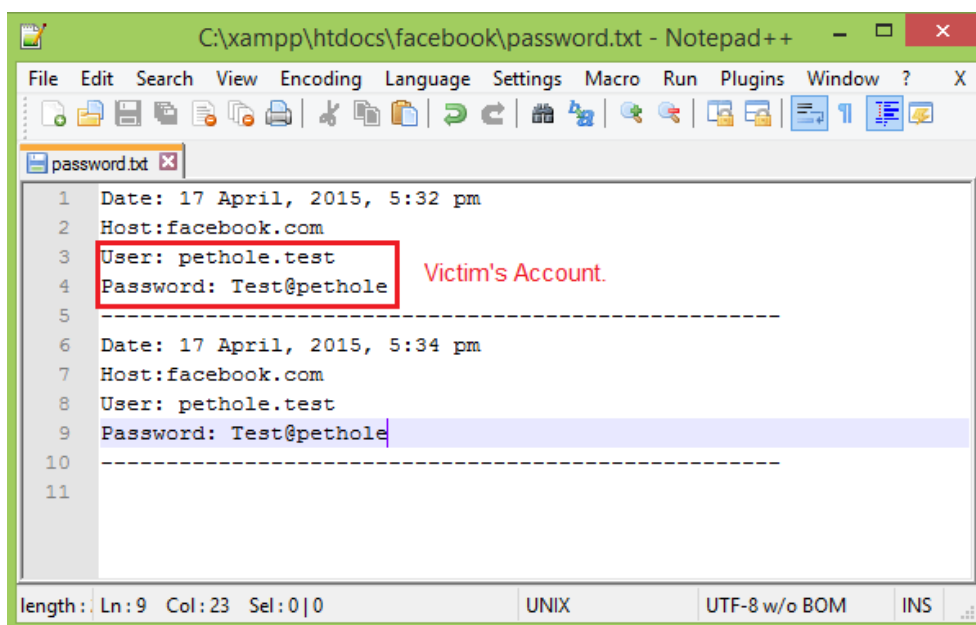
The research was conducted in 4 months, from December 2014 and divided into 3 phases: Identifying the scope of the research; Scanning every router's IP on our tool built for this project; Analyzing data and building tool to thoroughly fix the issue.

### Phase 1: Identifying scope of the research

**With holes:** Among many router vulnerabilities disclosed, we decided to focus on two critical holes which could help attackers easily take control of the devices. Many routers in Vietnam were affected, and we assumed a similar situation in the world.



The holes exist in backup of routers' configuration file. Normally, a configuration file should contain settings information, including password encrypted by weak algorithm. Hacker can download this file, then decrypt and get password of the router before taking control of it. Besides, some routers allow access to DNS configuration page without having to log in. Taking advantages of these holes, hacker can redirect router's DNS to his own server, then control all of users' communications with websites. Users are at risk of MitM attacks, Phishing attacks and might have their banking credentials, social networking, email accounts stolen.



```
C:\xampp\htdocs\facebook\password.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ? X
password.txt
1 Date: 17 April, 2015, 5:32 pm
2 Host:facebook.com
3 User: pethole.test
4 Password: Test@pethole
5 -----
6 Date: 17 April, 2015, 5:34 pm
7 Host:facebook.com
8 User: pethole.test
9 Password: Test@pethole
10 -----
11
length: Ln: 9 Col: 23 Sel: 0|0 UNIX UTF-8 w/o BOM INS
```

*Username and password of test Facebook account revealed in plain text*

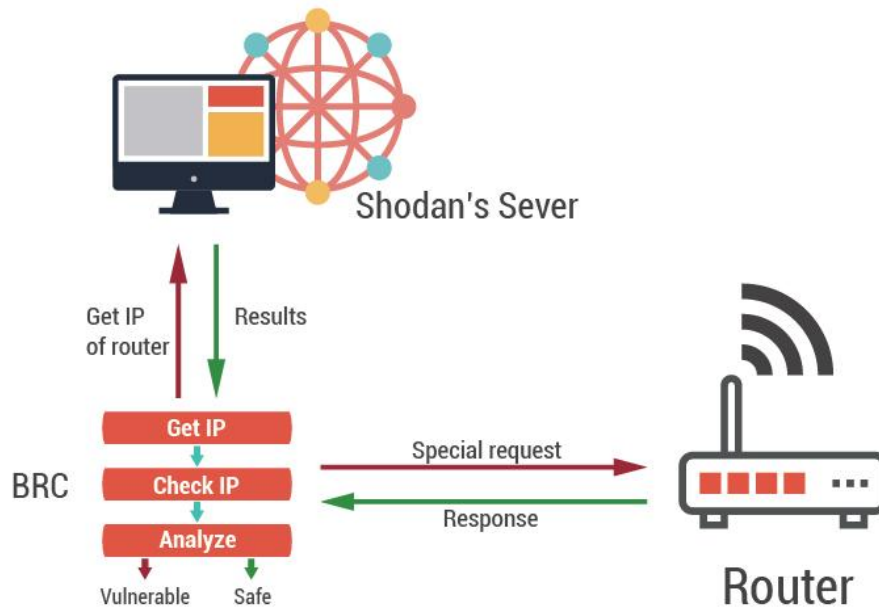
**With routers:** To ensure the most accurate outcome, we decided to check the existence of the holes in possible biggest samples, meaning all routers we could collect. We chose to use Shodan ([www.shodan.io](http://www.shodan.io)), a search engine that let users find specific types of computers (routers, servers, etc.) connected to the Internet. A global scale search was performed on Shodan, and the result we got was a list of 10,452,216 routers which might be vulnerable. To make it clear, “might be vulnerable” here means these routers are running platforms where the two holes reside. (*Note: To ensure no one takes advantage of this research to attack users, we will not specify the names of the holes. However, within this research, we provide a tool for users to easily check a router to be vulnerable or not when the names of the flaws are still unknown. We decide to stick with keeping the names secret because the two flaws have been long disclosed, once knowing the names hackers can Google them to find exploit code.*)

**Naming the issue:** We named the issue **Pet Hole** due to the fact that router is like a door leading users to the Internet. The door should be ensured with highest security, and despite users indeed close it, they unintentionally leave out the holes through which bad guys can intrude inside the system. This is like a Pet Door which is always open for our beloved dogs or cats to easily pass, but it is also a chance opened for attackers.



## Phase 2: Scanning every IP on our tool built for this project

To ensure accurate number of vulnerable routers without interfering in user's privacy, we built a system for this project. Dubbed Bkav Router Checker (BRC), the system does not retrieve routers' admin password, it only returns either YES or NO. YES means the router is vulnerable to attacks and NO means the router is safe.



*Bkav Router Checker operation*

**Phase 3: Analyzing data and building tool to thoroughly fix the issue**

From the data collected, we analyzed in different approaches to find out answers to pre-stated questions:

- The number of vulnerable routers
- The countries with highest number of unsafe systems
- Security of routers used in China, home of most routers in the world
- The list of vulnerable router models
- What the causes are and how to thoroughly fix the issue

Also, it's undeniable that despite many critical flaws have been unearthed, there is no fix yet to help users fully protect their routers. We decided to spend time and work out a tool to simplify the inherently complicated patching of routers.

## Key Findings

### 1. More than 1.4 millions of networks worldwide vulnerable to Pet Hole

1,437,192 is the number of router IPs which are flagged vulnerable by BRC. This means Internet connection of more than 1.4 millions of households and even businesses are at risk of being controlled by hackers. To help readers have a clear view of the impact, we prepared a table comparing Pet Hole with Heartbleed, the most notorious vulnerability of the year 2014.

Criteria	Pet Hole	Heartbleed
Severity	High	High
Rate of successful exploit	High	Medium
Impact	High	High
Required skill/knowledge for successful exploit	Basic knowledge of security	Expert knowledge of security
Patch	Difficult to patch	Quite easy to patch

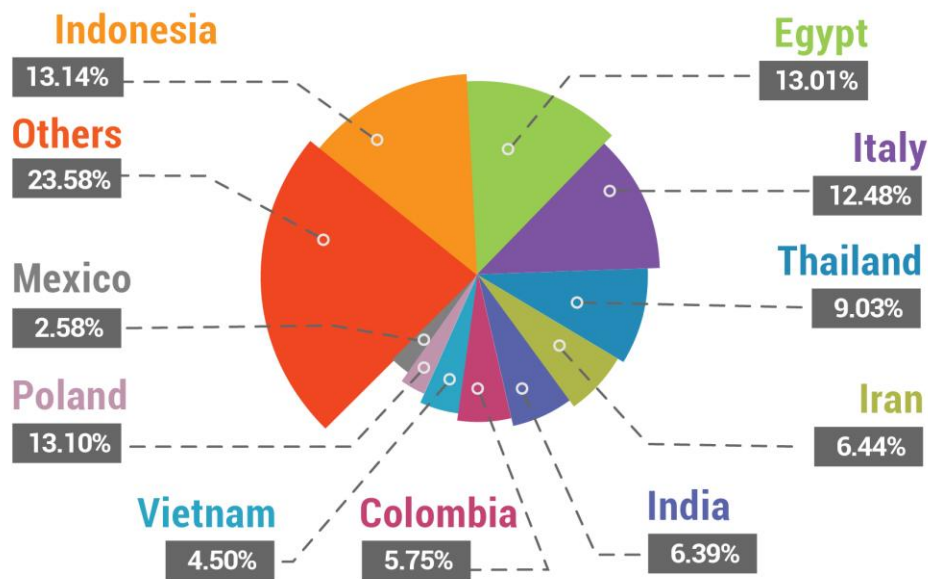
That's in theory, what about in reality? Let's see what happens in [this demonstration clip](#). (The clip records our laboratory experiment with a vulnerable router bought in Vietnam).

It's clear. Pet Hole is even more serious than Heartbleed. While Heartbleed requires expert knowledge in security to be successfully exploited, Pet Hole exploitation only needs basic skill. While it's easy to patch Heartbleed, patching Pet Hole is complicated. Furthermore, the clip has proved that Pet Hole is easy to be exploited in reality. To make sure, we even had a second year IT student participate in the experiment. With a few minutes of basic instructions, he could change the vulnerable router's DNS settings without any difficulties.



At the time of writing, more than 1.4 million networks have vulnerabilities in their routers, its impact is not small at all, if not a disaster in case a certain force is maintaining it for use in future.

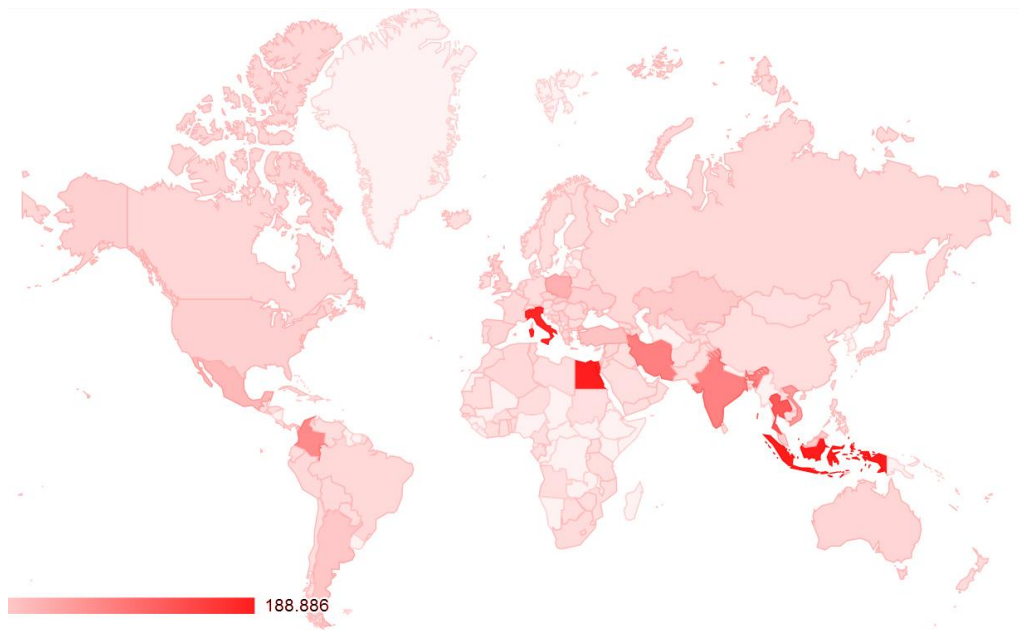
## 2. Indonesia, Egypt, Italy lead in number of vulnerable routers



*10 countries with highest number of vulnerable routers*

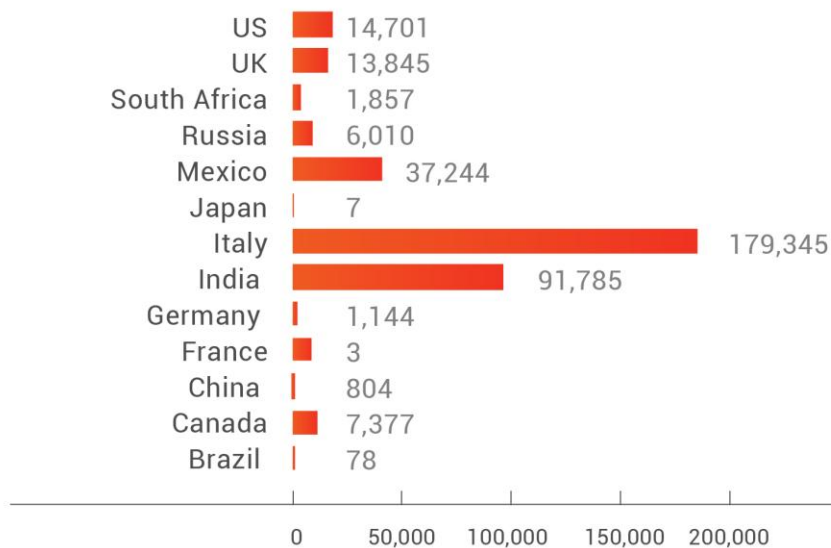
Indonesia ranks the 1<sup>st</sup> among 10 countries with highest number of vulnerable routers, 13.8% of Indonesia's routers (equivalent to 189 thousand devices) are at risk of being attacked via Pet Hole. Ranking 2<sup>nd</sup> and 3<sup>rd</sup> are Egypt (187 thousand routers) and Italy (179 thousands).

It is noteworthy that among this top ten, 5 are from Asia, while Europe has 3 nations and the Americas ranks 3<sup>rd</sup> with 2 nations. The result is quite equivalent to the development of technology in different continents in the world. Asia is a continent which develops quickly in the past decades, but such growth is not accompanied by the growth infrastructure, especially technology infrastructure. 5 nations of this continent appearing in this top 10 are all the ones with high number of Internet users [1]. Europe and the Americas have the highest development level of technology. Africa, in contrast, has no country in this top 10, which is simple to explain because until 2014 only 20% of this continent's people use the Internet [2].



*Geographical distribution of vulnerable routers*

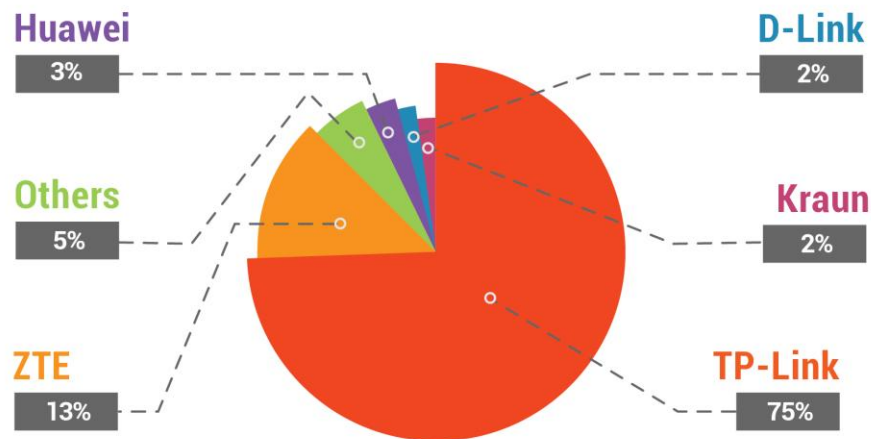
### 3. Most members of G8+5 not appear in top 10



As can be seen from the chart, most G8+5 members have a small number of vulnerable routers. Especially, Japan has only 7 despite the fact that this country is among the top 10 nations with biggest number of Internet users [1]. This is quite simple to understand. These are all developed nations, where management, including management in IT, is much better than in others, creating more secured systems.

Besides, most routers by Chinese manufacturers belong to low price segment, therefore being used widely in developing countries.

#### **4. More than 90% of vulnerable routers homed in China**



In the list of routers being at risk of Pet Hole, only Kraun and a very small number of other manufacturers are not from China. The rest, at least 93%, are from this country, with the names TP-Link, ZTE, Huawei and D-Link. Especially, 10 models which ranks top in terms of vulnerable device number are from TP-Link and ZTE, occupying more than 50% of system flagged insecure by BRC.

#### **5. China produces most but little routers in this country be vulnerable**

When analyzing the data collected by Bkav Router Checker, an issue captured our attention; that is China ranks 59<sup>th</sup> in terms of vulnerable devices. Specifically, 804 routers in this country are at risk of Pet Hole. It's far different from our initial expectation, because China has always owned a huge number of Internet users (ranking 1<sup>st</sup> in the world in 2014 with more than 600 hundred millions) [1]. Then, the number of vulnerable routers should have been huge too.

Trying to find out an explanation, we got another surprise when it turned out that among 10,452,216 routers running vulnerable platforms listed by Shodan, only 16,000 routers were from China. While Indonesia, a country with only 38 million Internet

users - 1/18 the number of China, has 153,182 routers in Shodan's database. Maybe, it's the actual situation in China that not many users there are using routers with vulnerable platforms; or China has implemented a special wall to protect its systems, making Shodan unable to interfere to create an accurate list. Nevertheless, the surprisingly low number of vulnerable routers in China is noteworthy.

## **Conclusions and Recommendations**

### **1. Conclusions**

Our research does not aim to uncover new vulnerabilities, but makes a report of routers around the world that are still vulnerable to critical ones despite the fact that people have known about them for months. The result is just like our initial expectations. The number of vulnerable routers is not small at all, while our research's subject is just 2 certain critical holes among many out there. It's certain that many other critical holes have not been discovered, or even might be silently exploited without user's concern. Router is the door connecting your network with the Internet. This door being unsafe means bad guys can invade into your house, or secretly sit on the entrance and keep track of your every move.

#### ***Why users not pay attention to this entrance?***

The first and easy-to-see, updating patch for router is not simple like updating for softwares. With softwares, users just need to follow usually uncomplicated instructions, or sometimes our systems automatically update themselves. Router update needs direct interference from users. Nevertheless, even when the instructions are as detailed as possible, not every user has enough knowledge of computer network to follow. Therefore, with routers used in households, the possibility that users leave out the hole is high. With businesses, where might exist IT unit, the update seems easier. The problem then lies right in the awareness of these IT people. In a business' network, a router might provide Internet connection for dozens or even hundreds of computers. Hence, the impact is not small even when there is only one business opens this door.

#### ***Security issue of devices from China***

We all know that most current routers are of Chinese manufactures, or at least are manufactured in this country. While, security issue relating to devices from China has long been a question with other nations. As by our research, more than 90% of the vulnerable routers are the products of Chinese manufacturers. Even though the likely reason might be that these are not high end devices, making them less secured; it is not unneeded that we pay more attention to security of devices from China.

***How is nation security threatened?***

Once again we need to mention that router is the entrance of our network, taking control of router means taking control of our system. More than 1.4 millions of devices being vulnerable to Pet Hole are not a small number. As described above, to successfully exploit Pet Hole is not difficult, even an amateur attacker can use it to intercept users' communications, redirect DNS to his website, etc. To a larger extent, if a nation has conspiracy to track other nations, it can totally carry out the scheme via this gateway.

**2. Fixing the hole**

Bkav has developed a tool for users to check the existence of Pet Hole in their router. Users just need to access [Checkrouter.net](http://Checkrouter.net), click on **Check** button, details of the routers will be displayed right below. If the router is vulnerable, there will be instructions to overcome the issue.

The first set of instructions lead users to quickly and simply disable access from the Internet, which is the primary attack vector used by hackers. Then, the “door” router has been closed, meaning the system is safe at least from the outside bad guys.

The best is to update the latest version for router's firmware. Step by step instructions are also available in [Checkrouter.net](http://Checkrouter.net).

Users can also go to Appendix 2 to see these detailed instructions.

After all actions have been completed, check the router again with our tool. If it is still vulnerable, then it's best that user buys another router.

## **About Bkav**

Established in 1995, Bkav Corporation is the leading firm in network security, software, smartphone manufacturing and smarhome. In the field of network security, antivirus and mobile security softwares of Bkav have been present in more than 100 countries all over the world. The leading technology research and advisory firm Gartner has listed Bkav among "Cool Vendors in Emerging Markets".

Bkav has preeminent security experts. The corporation is known as the security firm to discover the first critical flaw in Google Chrome just days after its launch in 2008. Bkav was also the firm to trace the master server in Britain of unprecedentedly massive DDoS attacks targeting US and Korean governments' websites in July, 2009.

Bkav Corporation is known as a manufacturer of security appliances such as intrusion prevention system Bkav Network Inspector, Bkav Antispam GW, Bkav WebSecurity Scan. Bkav is also providing collaboration software products (messenger, workflow management, mail, video conference).

In electronics industry, Bkav is a smartphone and smarhome manufacturer. With Bkav SmartHome, every equipment in your house will be connected and controlled automatically based on smart context scenarios via touch screen or tablet, hence creating a convenient, safe and energy-saving living environment.

### **Contact Information**

#### **Bkav USA**

800 El Camino Real, Mountain View, California, 94040

Telephone: (+1) 202 386 6779

Website: [www.bkav.com](http://www.bkav.com)

Email: [Bkav@bkav.com](mailto:Bkav@bkav.com)

## Appendixes

### Appendix 1: Routers experimented in Bkav's Lab

Manufacturer	Model	Specifications
TP-Link	TD-8840t	Production time: 2014 Firmware ver.: 22/10/2014 (latest)
	TD-W8951ND	Production time: 2014 Firmware ver.: 14/11/2014 (latest)
	TD-8817	Production time: 2014 Firmware ver.: 17/02/2013 (latest)
	TL-WR340G	Production time: 2014 Firmware ver.: 15/07/2011 (latest)
	TL-WA701N	Production time: 2014 Firmware ver.: 24/03/2014 (latest)
	TD-W8901	Production time: 2014 Firmware ver.: 14/11/2014 (latest)
Netis	WF-2420	Production time: 2014 Firmware ver.: 1/9/2014 (latest)
D-Link	DIR-615	Production time: 2014 Firmware ver.: 19.00 (latest)
	DSL-2640B	Production time: 2014 Firmware ver.: SEA_1.0 (latest)
Tenda	A5s	Production time: 2014 Firmware ver.: 2/5/2013 (latest)



### Appendix 2: Instructions to upgrade firmware & disable access from the Internet

– To upgrade firmware:

- Download the latest firmware version from the website of your router's manufacturer. (Do not use firmware from unclear origin because it might have been interfered to track user's activities, or it might destroy your device). [You can download here]
- Log in your modem's administration page via the gateway address from browser installed on a computer within the network (E.g. default gateway 192.168.1.1)
- Access firmware upgrade feature (normally it should be Maintenance or Management => Firmware)
- Click on "Choose file" or "Browse", then select the just-downloaded firmware.
- Choose "Upgrade" and wait for your router to reboot.

– To disable access from the Internet:

- Open a Command Prompt Window, Telnet to the router's gateway (E.g. telnet 192.168.1.1)
- Enter the admin password and execute commands as shown in the below picture.

```
C:\>telnet 192.168.1.1
Password: *****
Copyright (c) 2001 - 2013 TP-LINK TECHNOLOGIES CO. LTD
TP-LINK> sys server load _____ load current parameters into runtime memory
TP-LINK>
TP-LINK>
TP-LINK> sys server access web 2 _____ Setting remote over web (http)
TP-LINK> sys server save [0] Enable all.
sys server: save ok [1] Disable all.
TP-LINK> _ [2] Just remote in LAN.
Save setting [3] Just remote in WAN. (internet)
```

- With "Sys server access web" command, choose [1] or [2] to disable remote access from the Internet. In case you need frequent access to the admin page, you can choose to allow remote access via LAN only. If you don't need frequent access, Bkav recommends you disable the remote mode to protect your router against attacks from devices within your LAN network.

- Your router is now safe from attackers who attempt to attack your system from the Internet.

**Appendix 3: Vulnerable routers by country**

<b>No.</b>	<b>Country</b>	<b>Vulnerable routers</b>
1.	Indonesia	188,886
2.	Egypt	186,944
3.	Italy	179,345
4.	Thailand	129,833
5.	Islamic Republic of Iran	92,517
6.	India	91,785
7.	Colombia	82,623
8.	Vietnam	64,645
9.	Poland	44,496
10.	Mexico	37,244
11.	Turkey	27,074
12.	Argentina	24,020
13.	Kazakhstan	20,692
14.	Malaysia	16,840
15.	Slovakia	15,329
16.	United States	14,701
17.	United Kingdom	13,845
18.	Ukraine	13,720
19.	Armenia	10,549
20.	Bosnia and Herzegovina	9,953
21.	Spain	9,731
22.	Czech Republic	9,535
23.	Australia	9,424
24.	Greece	7,547
25.	Canada	7,377
26.	Tunisia	7,272
27.	Brazil	6,160
28.	Russian Federation	6,010

29.	Panama	5,605
30.	Azerbaijan	5,565
31.	Occupied Palestinian Territory	5,467
32.	Peru	5,389
33.	Republic of Moldova	5,389
34.	Belarus	5,232
35.	France	5,081
36.	Philippines	4,519
37.	Bolivia	4,382
38.	Syrian Arab Republic	4,009
39.	Algeria	3,976
40.	Romania	3,440
41.	Lebanon	3,093
42.	Finland	2,930
43.	South Africa	1,857
44.	Israel	1,759
45.	New Zealand	1,720
46.	Cuba	1,524
47.	Hungary	1,445
48.	Sri Lanka	1,445
49.	Uzbekistan	1,256
50.	Albania	1,249
51.	The Former Yugoslav Republic of Macedonia	1,203
52.	Germany	1,144
53.	Sweden	1,105
54.	Kyrgyzstan	955
55.	Belgium	863
56.	Pakistan	837
57.	Paraguay	804
58.	China	804

59.	Niger	772
60.	New Caledonia	765
61.	Mauritania	765
62.	Honduras	732
63.	Ecuador	713
64.	Lao People's Democratic Republic	706
65.	Morocco	693
66.	Georgia	693
67.	Cambodia	661
68.	Denmark	654
69.	Portugal	621
70.	Venezuela	602
71.	Ireland	589
72.	Netherlands	543
73.	Switzerland	497
74.	Singapore	399
75.	Ivory Coast	379
76.	Benin	334
77.	San Marino	288
78.	Bahrain	242
79.	Kuwait	203
80.	Afghanistan	183
81.	Maldives	177
82.	Saudi Arabia	150
83.	Cyprus	144
84.	Norway	144
85.	Liechtenstein	131
86.	Senegal	131
87.	Austria	131
88.	Sudan	124
89.	Lithuania	118

90.	Mauritius	118
91.	Cameroon	118
92.	Luxembourg	111
93.	Bangladesh	98
94.	Barbados	92
95.	Réunion	92
96.	Chile	85
97.	Djibouti	85
98.	Botswana	85
99.	Croatia	85
100.	Guadeloupe	78
101.	Bhutan	78
102.	Oman	72
103.	Brunei Darussalam	65
104.	Malta	59
105.	Gibraltar	59
106.	Tajikistan	59
107.	Bermuda	52
108.	Angola	52
109.	Vanuatu	33
110.	Mozambique	33
111.	Gabon	33
112.	Costa Rica	26
113.	Faroe Islands	26
114.	Yemen	26
115.	Guatemala	26
116.	Taiwan, Province of China	26
117.	Comoros	20
118.	Estonia	20
119.	Burkina Faso	20
120.	El Salvador	20

121.	Dominican Republic	20
122.	Fiji	20
123.	Zimbabwe	20
124.	Martinique	13
125.	Uganda	13
126.	Åland Islands	13
127.	Mongolia	13
128.	Iraq	13
129.	French Polynesia	13
130.	United Republic of Tanzania	13
131.	Iceland	13
132.	Bulgaria	13
133.	Jordan	7
134.	Ghana	7
135.	Libyan Arab Jamahiriya	7
136.	Timor-Leste	7
137.	United Arab Emirates	7
138.	French Guiana	7
139.	Togo	7
140.	Saint Kitts and Nevis	7
141.	Lesotho	7
142.	Japan	7
143.	Hong Kong	7

## References

- [1] The data concerning Internet users is taken from <http://www.internetlivestats.com/internet-users-by-country/>, in which the numbers are calculated using penetration rate (International Telecommunication Union - ITU) and population data from U.S. Census Bureau.
- [2] *The world in 2014, ICT Facts and Figures* by ITU <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf>
- [3] *Percentage of Individuals using the Internet* by ITU [http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals\\_Internet\\_2000-2013.xls](http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls)
- [4] Heartbleed details <http://heartbleed.com/>