# Annual Global Census on “Heartbleed” Vulnerability

## 1. Summary

On April 7th, 2014, a major vulnerability (CVE-2014-0160) in the open source network security cryptography library OpenSSL was revealed (first discovered by engineers at Codenomicon and Google Security). Since this vulnerability may lead to the disclosure of server data which contains user’s sensitive information including username and passwords, it was given a vivid name “Heartbleed”.

On the very day of one year after “Heartbleed” outbreak, Knownsec ZoomEye Team carried out the regression census of the whole IPv4 space. Compared with last year, the influenced IP addresses have decreased to 14.6% by amount. However, a large number of vulnerable IP addresses (377,221) still exist.

Considering we’ve left enough time for engineers to debug, this report will release 1,000 affected IP addresses, hoping to arouse security awareness of the relevant personnel and improve the defense capability of cyber space.

## 2. Review

“Heartbleed” can be absolutely regarded as an epic vulnerability, which can be illustrated by the following data:

2.1 The affected IP addresses were most widespread. After carrying out the entire network scanning for HTTPS (443), IMAPS (993), SMTPS (465), and POP3S (995), ZoomEye Team have found that the number of affected IP addresses is 2,590,351 (2,433,550 after removing the overlapped ones). The global geographical distribution is shown below:

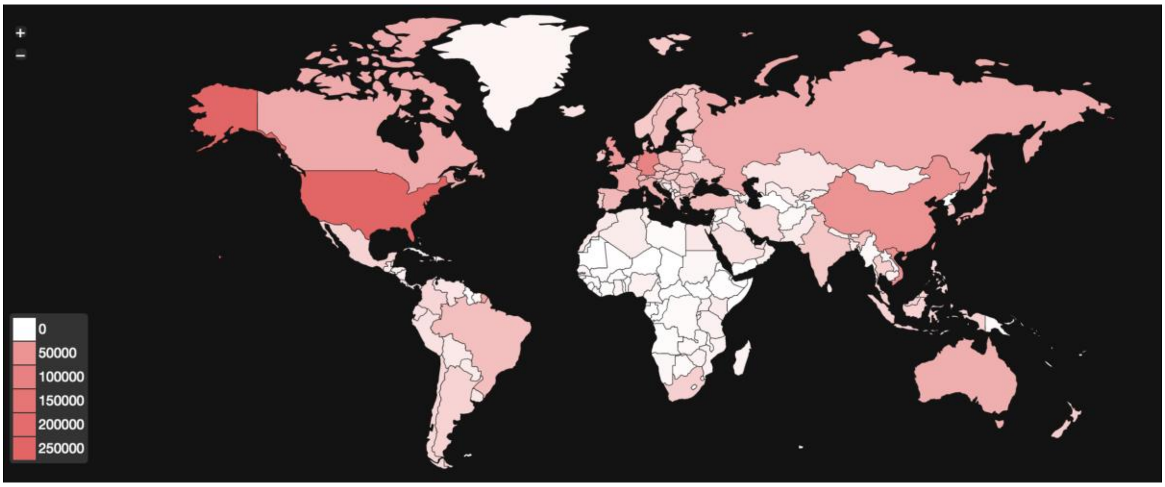

Figure 1: “Heartbleed” global distribution in 2014

According to the affected protocols:

- HTTPS (443): 1,772,058 (68.5%)
- IMAPS (993): 353,310 (13.6%)
- SMTPS (465): 104,792 (4.0%)
- POP3S (995): 360,191 (13.9%)

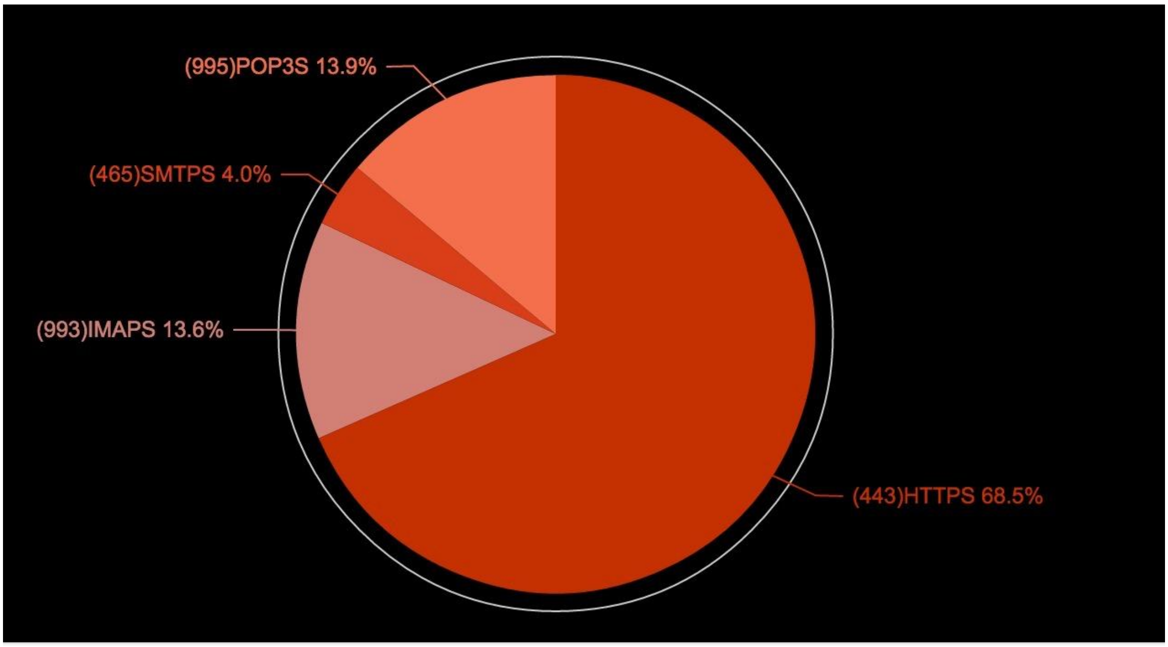

Figure 2: “Heartbleed” affected protocols distribution in 2014

The top 25 affected countries/regions in 2014 are:

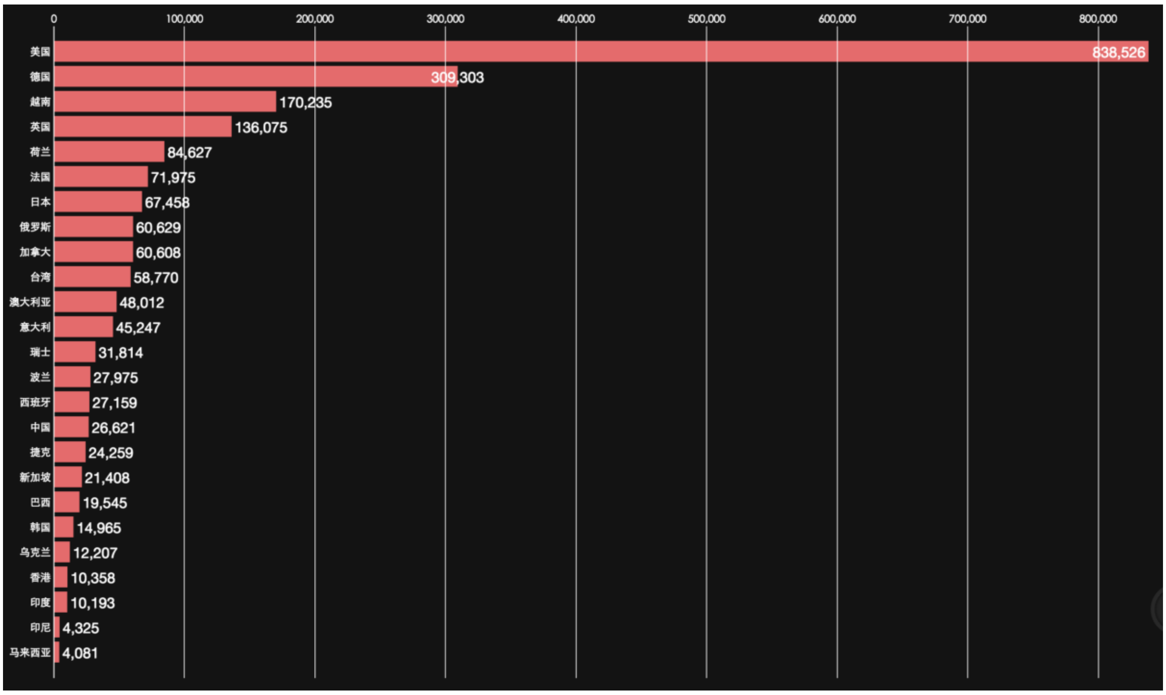

Figure 3: “Heartbleed” affected countries/regions in 2014

2.2 The impact is significant. Popular websites such as Facebook, Yahoo, Taobao, Alipay, JD and well-known manufactures such as Cisco (routers), Juniper (firewalls) and Legendsec (VPN gateways) are all on the list.

2.3 Responded most rapidly nationwide, ZoomEye Team continuously focused on the affected IP addresses. At the first 3-day interval, the global recovery rate is reaching a staggering 40%. But the repair rate in China is 18%, ranked only 102 in the world.

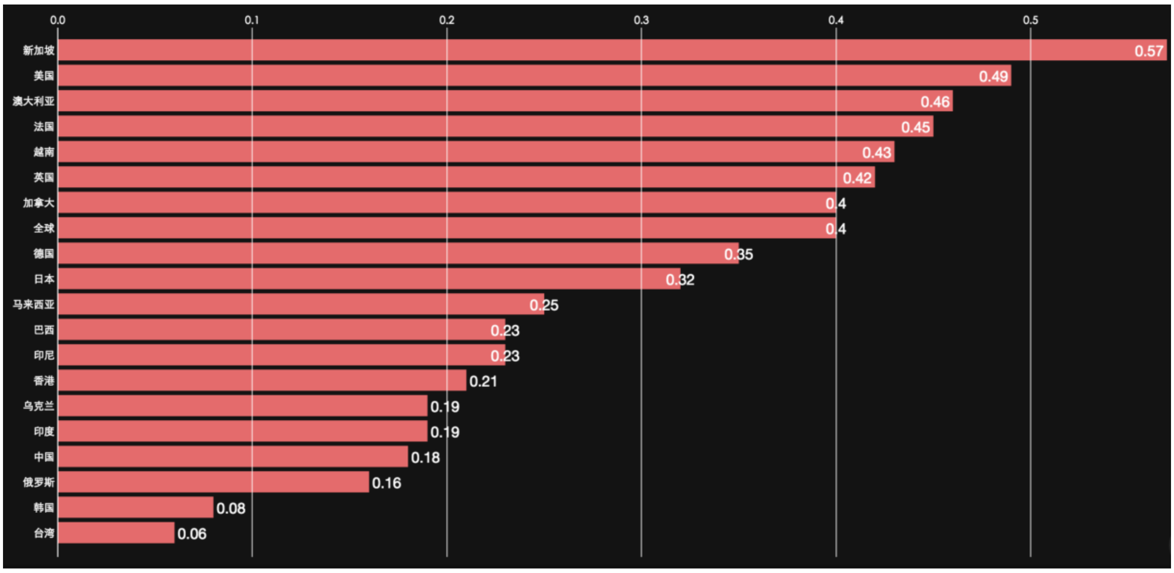

Figure 4: “Heartbleed” repair rate of 20 countries within 3 days in 2014

## 3. Annual Data Analysis

After one year's effort, ZoomEye Team carried out a regression global census. Comparing the two sets of data, some inspirations can be obtained as follows:

3.1 ZoomEye Team carried out the scanning task for the whole network IPv4 space including HTTPS (443), IMAPS (993), SMTPS (465) and POP3S (995) and found the number of affected IP addresses is 377,221. The non-repair rate is only 14.6% of the previous year. The global geographical distribution is shown below:

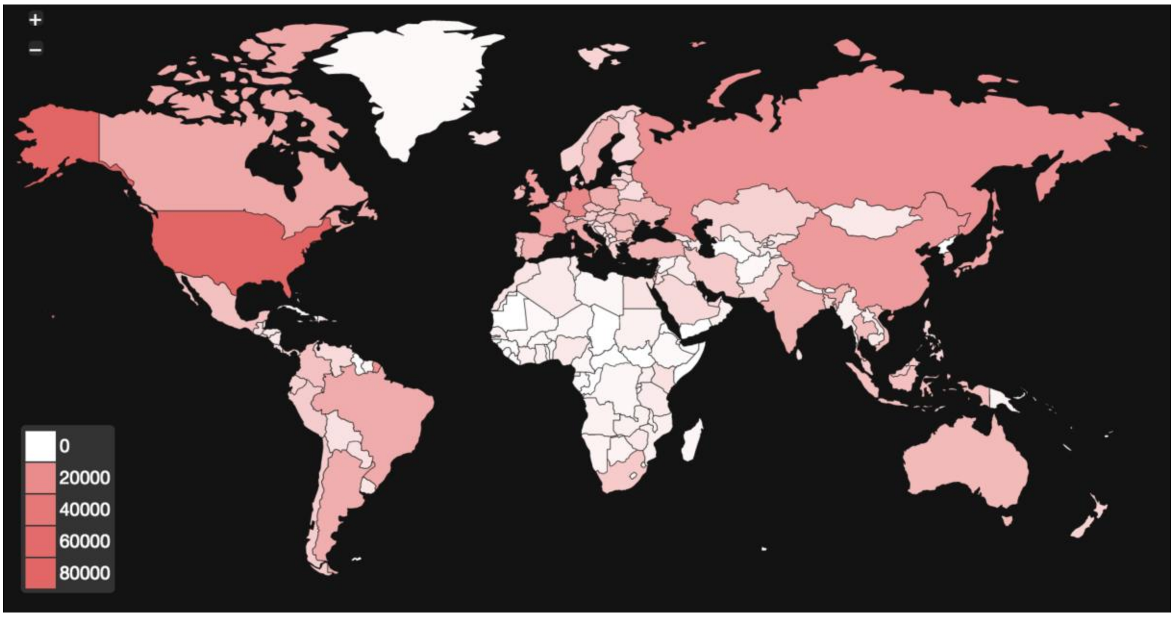

Figure 5: "Heartbleed" global distribution in 2015

According to the affected protocols:

- HTTPS (443): 199,495 (52.9%)
- IMAPS (993): 73,096 (19.4%)
- SMTPS (465): 36,044 (9.6%)
- POP3S (995): 68,586 (18.1%)

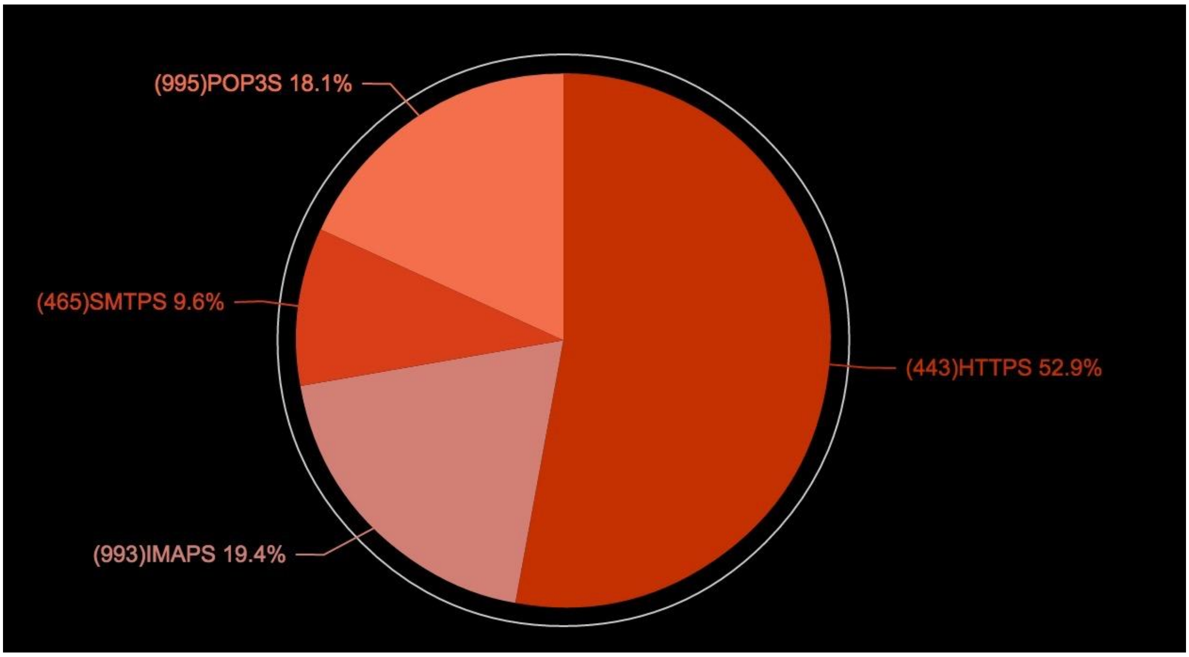

Figure 6: “Heartbleed” affected protocols distribution in 2015

The top 25 affected countries/regions in 2015 are:

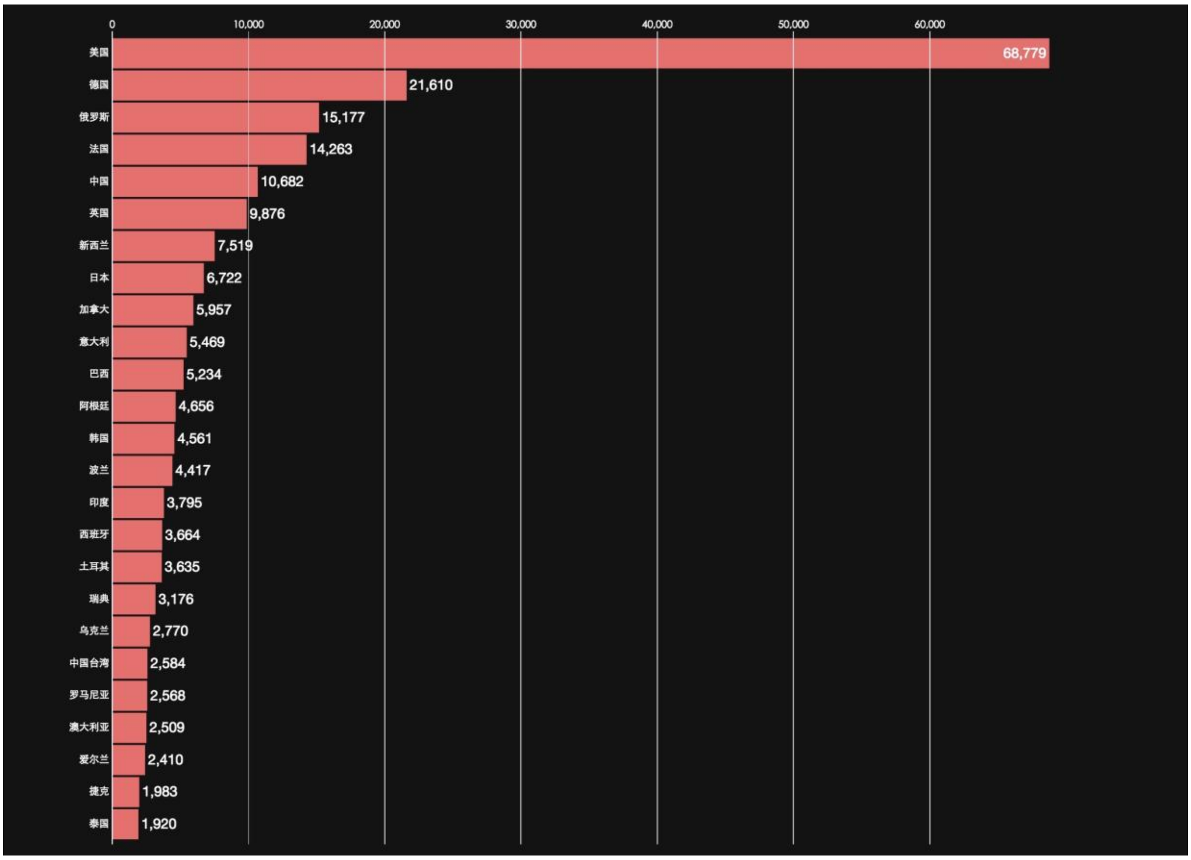

Figure 7: “Heartbleed” affected countries/regions in 2015

## 3.2 Sampling tests show popular websites such as Facebook, Yahoo, Taobao, and Alipay

have a high repair rate. No related bugs was found.

3.3 Annual continued responding speed:

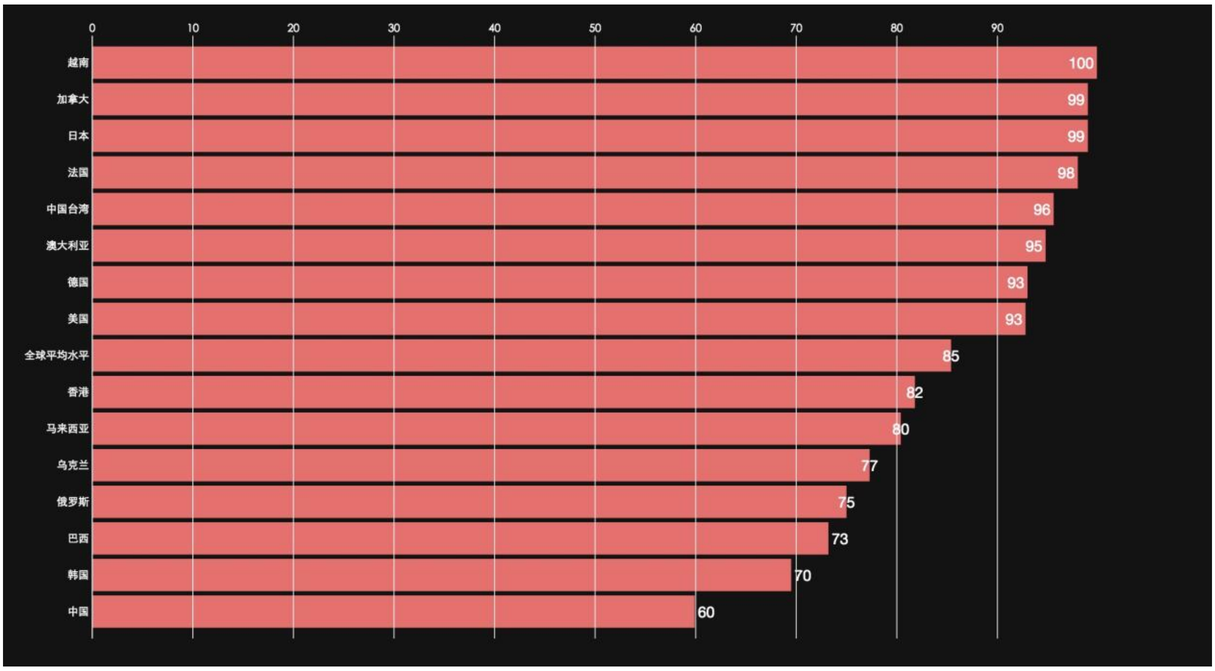

Figure 8: "Heartbleed" vulnerability repair rate of 16 countries in 2015

## 4. Conclusion

Compared with data a year ago, the following conclusions can be made:

4.1 Global debugging is efficient. The amount of affected global IP addresses has decreased to 14.6% of the previous year.

4.2 The affected IP addresses are protocol-dependent. For example, the amount of affected HTTPS (443) has reached over 50% of the overall affected IP addresses twice.

4.3 Debugging ability of developed countries is much more efficient than that of developing countries. Since developed countries have more IP resources (1/3 belonged to America), they account for the majority on the Top 25 Affected Countries/Regions List. However, after a year's rehabilitation, developing countries such as China, India, and Russia has emerged on the list of 2015.

4.4 As large websites such as Facebook, Yahoo, Taobao, Alipay, and JD paid more attention to security issues, no related bugs was found in sampling.

4.5 The continued responding capability of Mainland China still needs to be improved. Although the repair-rate has reached 59.9% from 18% a year ago, the cyber security defense capability remains a serious concern compared with Korea (69.5%), Russia (78%), Hong Kong, China (81.8%), Taiwan, China (95.6%), and Japan (99%).

Click here for more details.