KASPERSKY lab

KASPERSKY DDOS INTELLIGENCE REPORT Q3 2015

Contents

Q3 events

Of all the Q3 2015 events in the world of DDoS attacks and the tools used to launch them, we picked out those that, in our opinion, best illustrate the main trends behind the evolution of these threats.

- DDoS attacks targeting financial organizations for the purpose of extortion;
- new techniques to increase the intensity of attacks by manipulating web pages;
- active development of Linux-based botnets for DDoS attacks.

Attacks on financial organizations

In Q3 2015, there was increased activity by the cybercriminal group "DD4BC" responsible for a number of attacks on major banking organizations around the world. The group has been targeting banks, media groups and gaming companies since September, threatening to take down their customer websites unless they pay a ransom. The owner of the targeted resource is asked to pay between 25 and 200 bitcoins ($6,500 – $52,500), or have their servers disabled. Some of the first victims included organizations in Australia, New Zealand and Switzerland, while a warning was received by major financial institutions in Hong Kong. The Bank of China and the Bank of East Asia also reported that they were targeted by illegal activity. In the third quarter, a number of Russian financial institutions also received notifications from cybercriminals asking for a specific sum in cryptocurrency to terminate an attack.

Unusual attack scenario

The company CloudFlare reported a DDoS attack with an unusual scenario. A site belonging to one of CloudFlare's customers was being subjected to an attack made up of 275,000 HTTP requests per second. Of particular interest was the fact that the attackers made use of malicious JavaScript embedded in adverts. An iframe with a malicious advert that contained the JavaScript was run on the browsers of lots of users, resulting in their workstations sending XHR requests to the victim. Experts believe that these malicious ads can also display some legitimate applications.

XOR DDoS bot activity

The specialists at Akamai Technologies witnessed growth in the capacity of a DDoS botnet consisting of Linux-based computers whose victims were mostly Asian sites belonging to educational institutions and gaming communities. A distinctive feature of the bot is the use of XOR-encryption both in the malicious program and for communication with the C&C servers. At the same time, in order to self-propagate the bot brute-forces passwords to the root account in Linux systems. Linux is often used as a server operating system, which means that the server also has the channel and computing resources that the attackers can use to launch DDoS attacks. Using SYN and DNS floods, this botnet has been successfully carrying out attacks with a capacity of 109-179 Gbps.

According to Kaspersky Lab data, the botnets from Linux-based servers infected by the XOR DDoS bot actively attacked resources located in China.

DDoS availability

On the one hand, the software that is used for DDoS attacks is becoming more complicated; on the other hand, the tools for DDoS attacks are becoming more freely available and easier to use. As a result, setting up and launching a DDoS attack no longer requires any special technical knowledge. A fairly competent criminal could easily unleash a powerful attack.

This fact is confirmed by attacks on the educational portal of the Republic of Tatarstan carried out by students attempting to block communication between teachers and parents. Throughout the year the attackers repeatedly tried to bring down the portal, which was protected by Kaspersky DDoS Protection. All their attempts were unsuccessful, but their persistence did succeed in attracting the attention of Kaspersky Lab's experts.

The availability and ease of use of the tools for DDoS attacks has resulted in the range of targets growing. It is generally accepted that DDoS attacks are mainly focused on financial institutions, government agencies, businesses and the media. Now, however, any resource that has attracted the ire of an unscrupulous web user could be subjected to a DDoS attack – even an educational portal.

Statistics of botnet-assisted DDoS attacks

Methodology

The DDoS Intelligence system (part of Kaspersky DDoS Protection) is designed to intercept and analyze commands sent to bots from command and control (C&C) servers, and does not have to wait until user devices are infected or cybercriminal commands are executed in order to gather data.

In this report, a single (separate) DDoS attack is defined as an incident during which any break in botnet activity lasts less than 24 hours. If the same web resource was attacked by the same botnet after a break of more than 24 hours, this is regarded as a separate DDoS attack. Attacks on the same web resource from two different botnets are also regarded as separate attacks.

The geographical distribution of DDoS victims and C&C servers is determined according to their IP addresses. In this report, the number of DDoS targets is calculated based on the number of unique IP addresses reported in the quarterly statistics.

It is important to note that DDoS Intelligence statistics are limited to those botnets that were detected and analyzed by Kaspersky Lab. It should also be highlighted that botnets are just one of the tools used to carry out DDoS attacks; therefore, the data presented in this report does not cover every DDoS attack that has occurred within the specified time period.

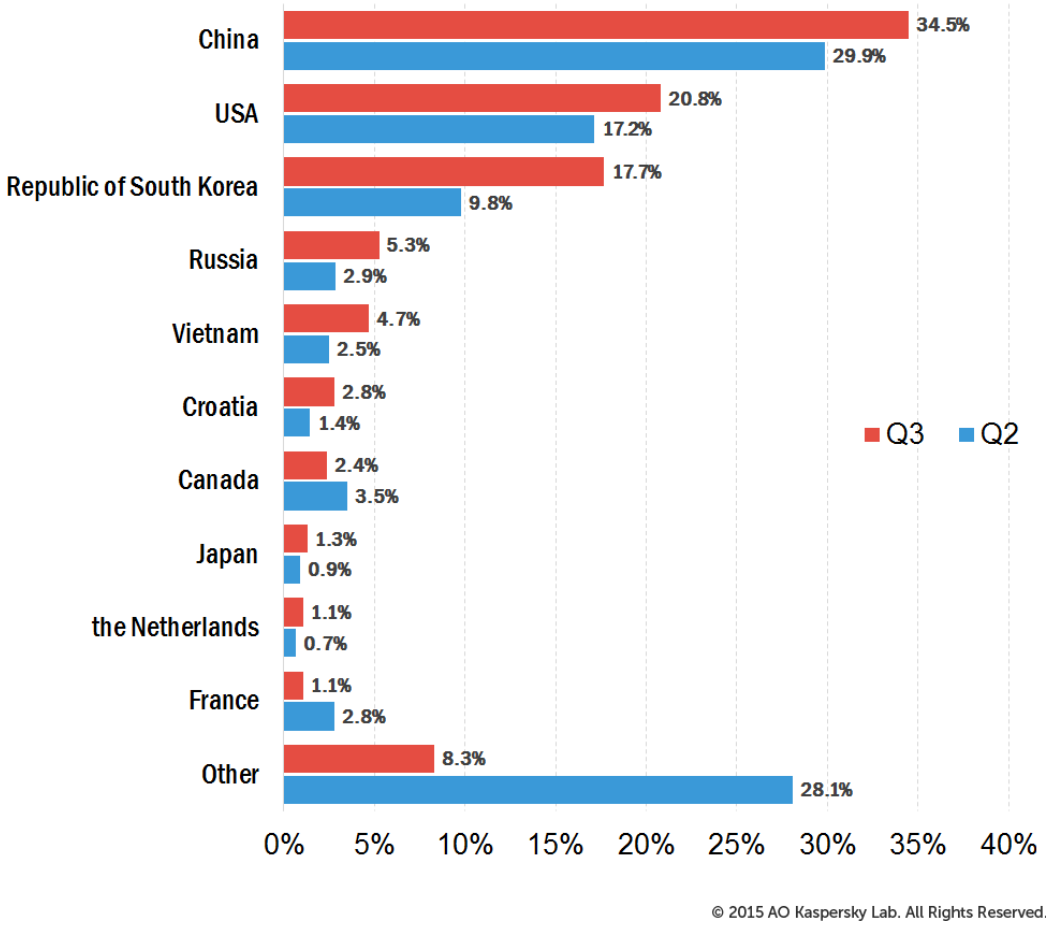
Q3 Summary

- In Q3 2015, botnet-assisted DDoS attacks targeted victims in 79 countries around the world.
- 91.6% of targeted resources were located in 10 countries.
- The largest numbers of DDoS attacks targeted victims in China, the US and South Korea.
- The longest DDoS attack in Q3 2015 lasted for 320 hours (or 13.3 days).
- SYN DDoS, TCP DDoS and HTTP DDoS were the most common DDoS attack scenarios.

- Linux-based bots are actively used by cybercriminals; the proportion of DDoS attacks from Linux-based botnets in the third quarter was 45.6%.

Geography of attacks

In Q3, the **targets of DDoS attacks** were located in 79 countries around the world. 91.6% of attacked resources were located in 10 countries.

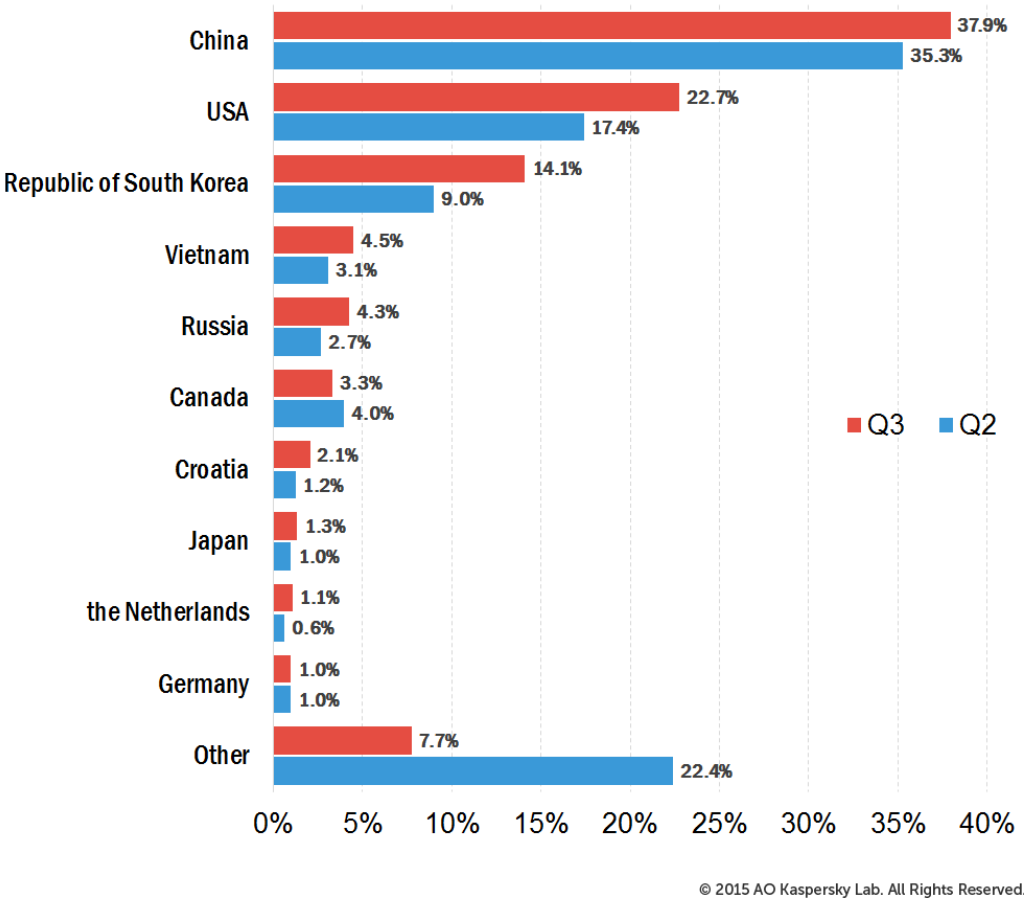


Distribution of unique DDoS attack targets by country, Q3 vs Q2 2015

China still leads the Top 10 ranking: in Q3 of 2015, 34.5% of DDoS attack targets were located there, an increase of 4.6 percentage points (p.p.) on the previous quarter. The US came second with 0.8%. South Korea remained in third place (17.7%) although its share increased considerably – by 7.9 p.p.

The Netherlands (1.1%) re-entered the Top 10. A newcomer to the rating was Japan whose share accounted for 1.3% of all attacked resources. Germany (1.0%) and Hong Kong (0.9%) left the Top 10.

If we look at the **number of reported attacks**, 92.3% of all attacks (an increase of 14.7 p.p. on Q2) had targets within the same Top 10 countries:



Distribution of DDoS attack by countries, Q3 vs Q2 2015

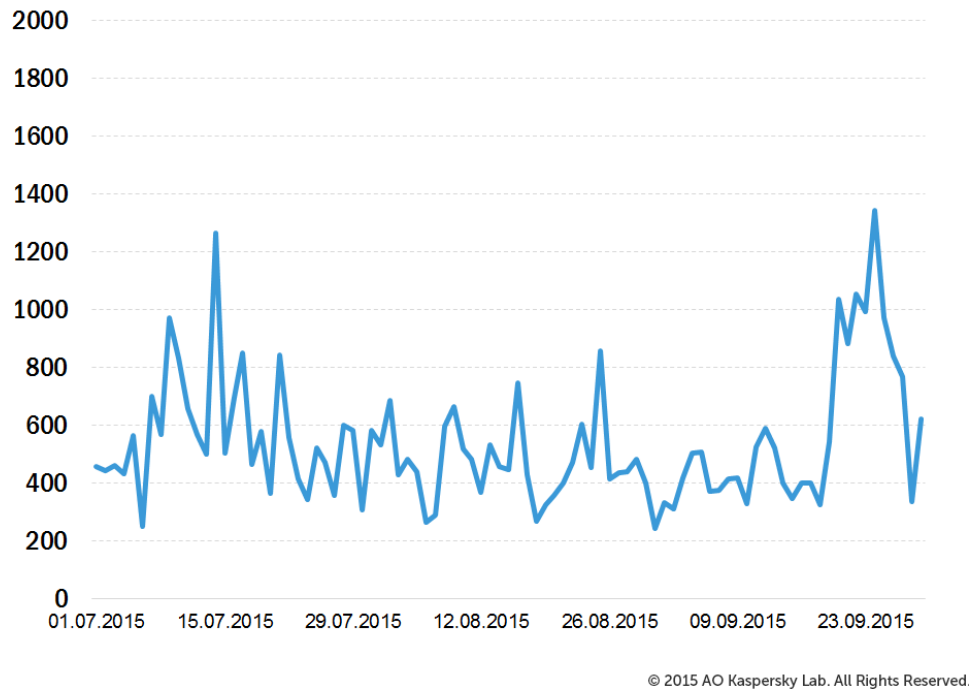
In the third quarter, China (37.9%), the US (22.7%) and South Korea (14.1%) remained in the leading three places. The Netherlands (1.1%) and Japan (1.3%) pushed France (0.9%) and Hong Kong (0.9%) out of the Top 10 in terms of the number of attacks. The biggest increase in the proportion of DDoS attacks in Q3 was observed in the US – the share of attacks grew by 5.4 p.p.

The figures for the leading three countries in both rankings – the number of attacks and the number of targets – increased by more than they did for the other Top 10 countries. The continued leadership of China and the US in the rankings is due to cheap web hosting in those countries, which explains why so many targeted web resources are located there.

The absolute leader in terms of the number of attacks was an IP address allegedly belonging to a data center in Hong Kong: throughout the quarter it was attacked 22 times.

Changes in DDoS attack numbers

In Q3 2015, DDoS activity was distributed unevenly, with two peaks: the first fell in mid-July, the second in late September. The quietest period was from early August to mid-September.

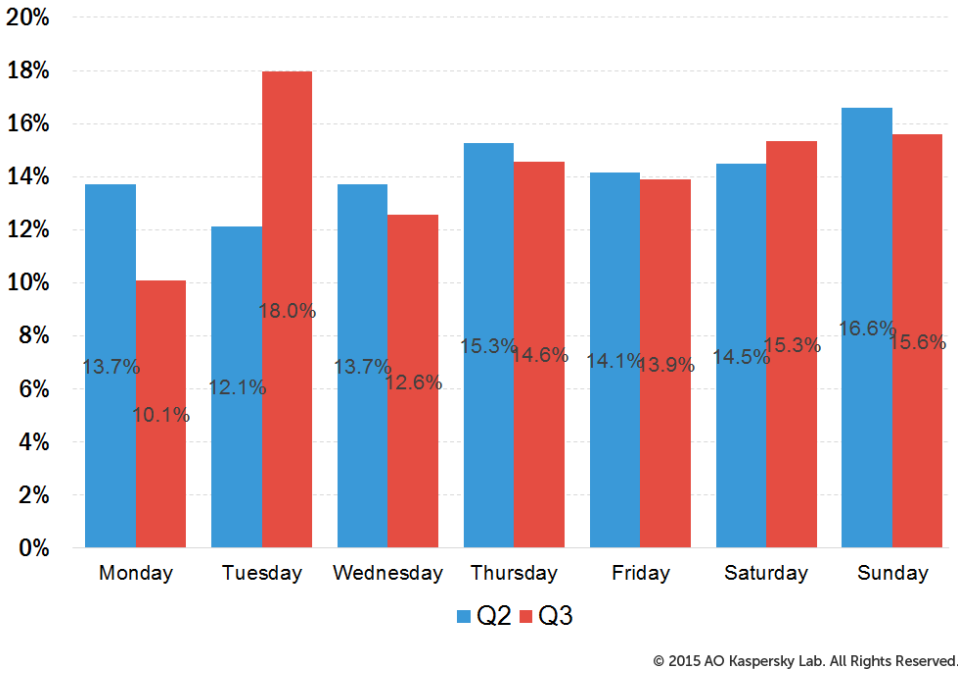


Number of DDoS attacks over time in Q3 2015.*

** DDoS attacks may last for several days. In this timeline, the same attack may be counted several times, i.e. one time for each day of its duration.*

The peak number of attacks in one day was 1344, recorded on 24 September.

Tuesday was the most active day of the week in terms of DDoS attacks.



Distribution of DDoS attack numbers by days of the week

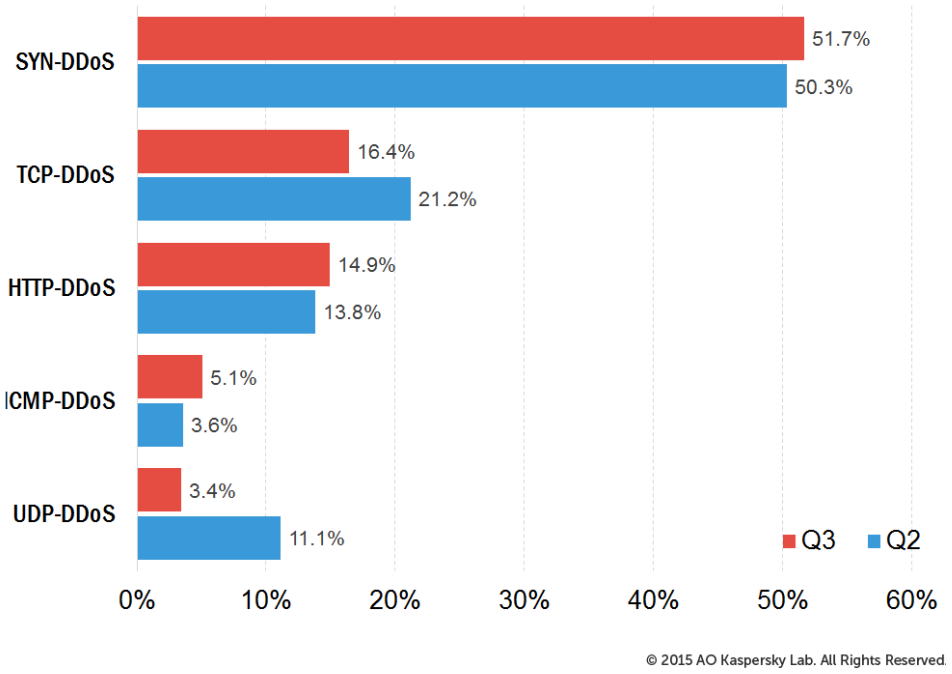
The fact that Tuesday leads is probably due to a dramatic rise in the number of DDoS attacks on that day of the week on 14 July and on 22 September. Particularly active on those two days were botnets from Linux-based servers infected by the XOR DDoS bot that attacked resources in China.

Types and duration of DDoS attacks

99.3% of DDoS targets in Q3 2015 (vs. 98.2% in Q2) were attacked by bots belonging to one family.

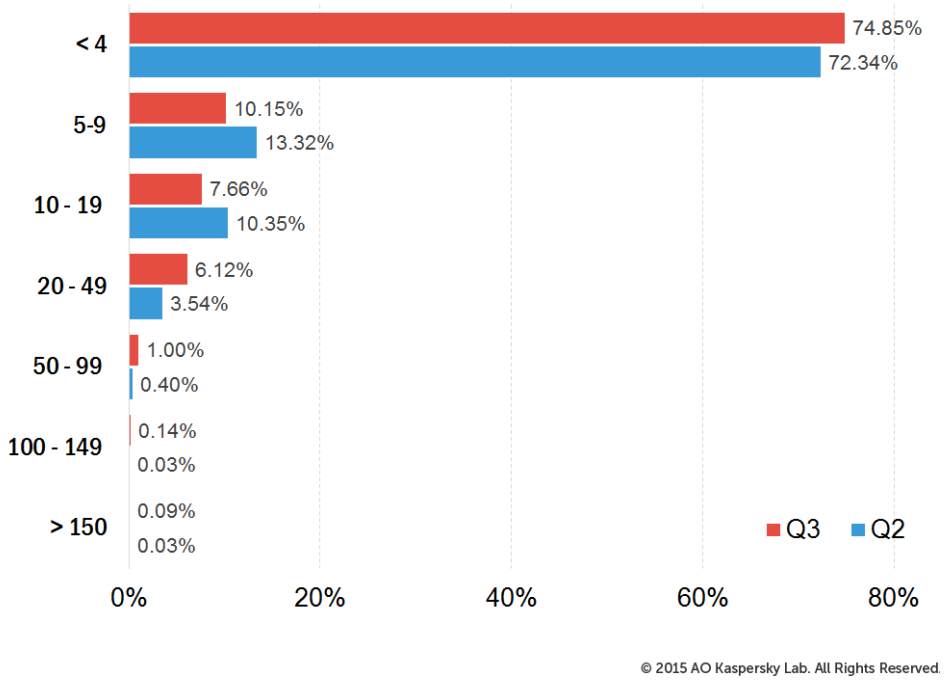
In only 0.7% of all cases cybercriminals launched attacks using bots from two different families (or the clients used the services of several attack agents). In 0.2% of cases, three or more bots were used.

In Q3 2015, SYN DDoS (51.7%) remained the most popular attack method. TCP DDoS (16.4%) and HTTP DDOS (14.9%) were second and third respectively. ICMP-DDoS, whose contribution doubled over the last two quarters and accounted for 5.1%, was fourth.



The distribution of DDoS attacks by types

Once again, most attacks lasted no longer than 24 hours in Q3 2015. However, the number of attacks that lasted a week or longer increased considerably.



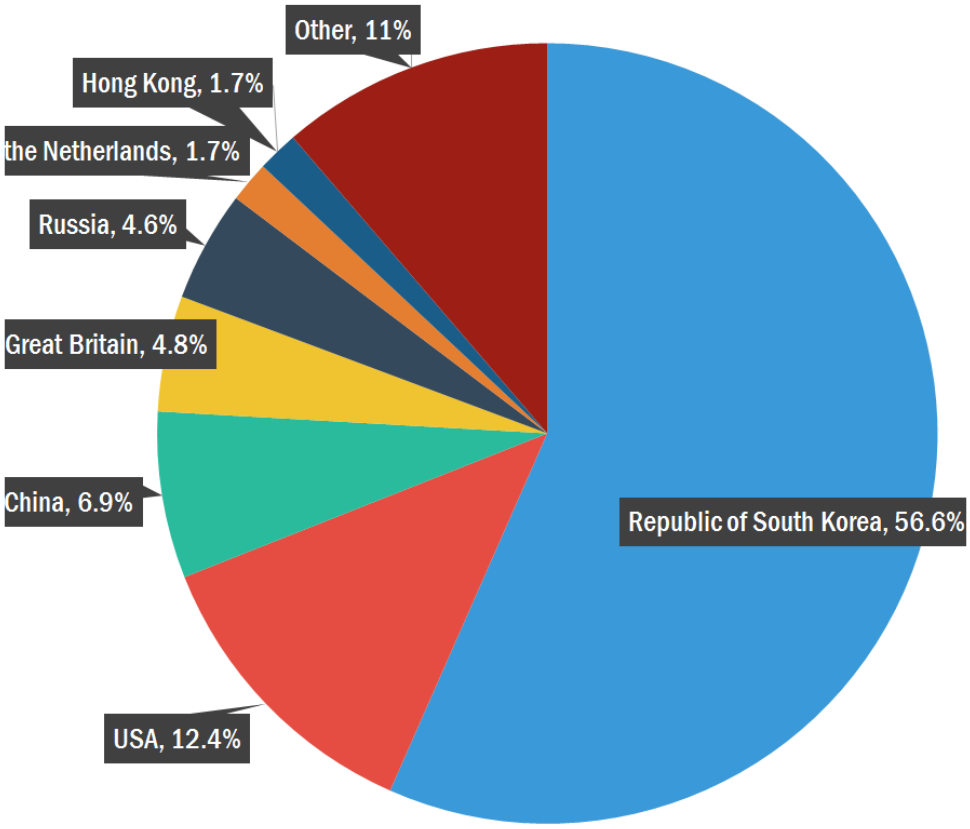
The distribution of DDoS attacks by duration (hours)

The longest DDoS attack in the previous quarter lasted for 205 hours (8.5 days); in Q3, this record was beaten by an attack that lasted 320 hours (13.3 days).

C&C servers and botnet types

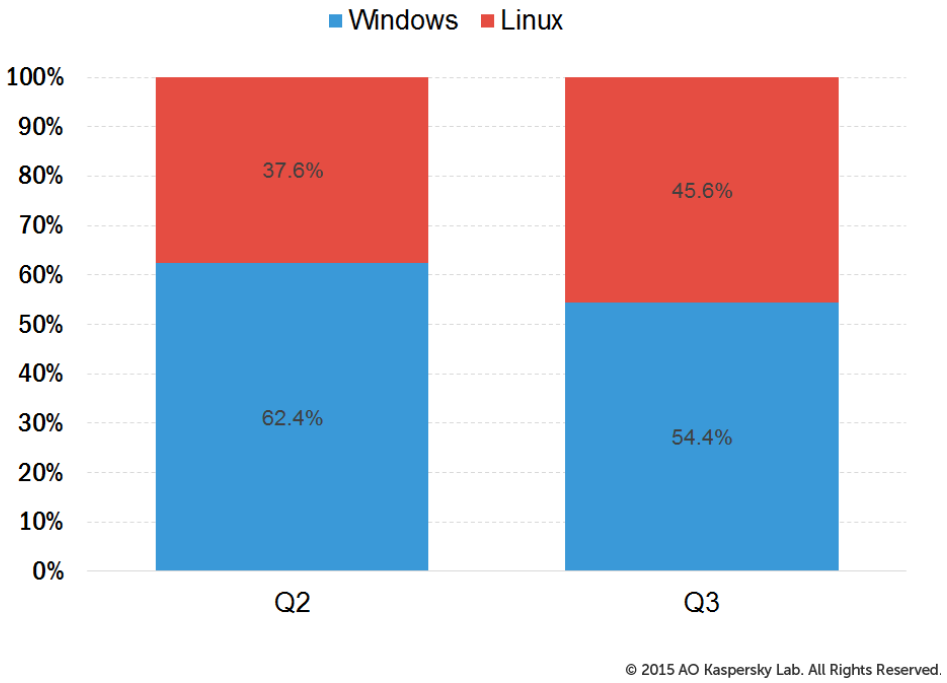
In Q3 2015, South Korea took the lead in terms of the number of C&C servers located on its territory; its share grew from 34% to 56.6%. Noticeably, in South Korea this quarter the number of C&C servers that control Nitol bots increased significantly. Nitol began to use Dynamic DNS services more actively, in particular, no-ip.org and codns.com. As mentioned above, the percentage of DDoS attacks targeting resources located in South Korea also increased.

The proportion of C&C servers located in the US and China dropped significantly – from 21% to 12.4% and from 14% to 6.9% respectively.



Distribution of botnet C&C servers by countries in Q3 2015

The activity of Windows and Linux botnets continued to fluctuate. After the previous quarter's reduction in the share of Linux-based botnets, in Q3 they regained ground – the proportion of attacks by Linux bots grew from 37.6% to 45.6%.



Correlation between attacks launched from Windows and Linux botnets

The increase in the proportion of Linux bot activity was most probably down to insufficient protection for Linux-based machines and, quite importantly, their higher Internet speeds. This makes Linux more attractive to cybercriminals despite the relative complexity in developing, acquiring and exploiting Linux bots.

Attacks on banks

The third quarter of 2015 saw the return of DDoS extortionists to the cybercrime scene. A number of major banking institutions in a variety of countries were targeted by DDoS attacks that were then followed by demands for a large payment in cryptocurrency to stop the attack. This particular aspect of the attacks suggests they are the work of the cybercriminal group DD4BC (Distributed Denial of Service for Bitcoin), which demands bitcoin ransoms.

It appears the group has now reached Russia, where a number of financial institutions were also attacked. Some of the Russian banks that were targeted were either protected by Kaspersky DDoS Protection or quickly connected to the service as soon as the DDoS attacks began. This meant they avoided any damage and the banks' websites and online banking systems continued to function smoothly.

Kaspersky Lab registered a wave of lengthy DDoS attacks on the online banking systems of eight well-known financial institutions, with some banks repeatedly targeted.

For all attacks the cybercriminals used a complex combination of amplification attacks that disable online resource with minimal effort.

Three types of attack were used to overload the channel: NTP amplification, SSDP amplification and RIPv1 amplification which reached 40 Gbps. In some cases, the attacks were supplemented by a HTTPS flood attack that reached 150 Mbps from a botnet with about 2,000 attacking hosts.

The attacks lasted from one to four hours.

The attackers not only demanded a bitcoin ransom but also threatened the banks with unprecedented terabit attacks. However, these threats have not been implemented in practice.

We can assume that the peak attack parameters registered at the end of September were the attackers' maximum – Kaspersky Lab experts recorded this particular aggregate capacity in simultaneous attacks on several banks.

Unfortunately, this does mean the power of attacks will not increase in the future.

Conclusion

The correlation between the number of attacks launched from Windows and Linux botnets marks an interesting trend, with criminals starting to actively use botnets from infected servers. There are several reasons for this.

Firstly, servers have a significantly bigger Internet channel than domestic machines, making it possible to organize powerful attacks with only a few C&C servers.

Secondly, the level of server protection is not always very high, leaving them vulnerable to hacking. If security patches are not regularly installed on the server, it quickly becomes an easy prey for cybercriminals: it does not take them long to discover such servers and exploit any known vulnerabilities. Then there is the expanded arsenal of available exploits that have appeared after a number of vulnerabilities were detected in open-source products such as exploits for the ghost vulnerability, which is still in use.

Thirdly, the power of a server botnet can be increased by renting additional servers.

In these circumstances, timely installation of security patches on servers becomes critical. For the owners of web resources, effective protection from DDoS attacks originating from server botnets is strongly recommended.

About Kaspersky Lab

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997 Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide.

Learn more at www.kaspersky.com.

Securelist the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy

KASPERSKY lab