The background of the page is a dark blue gradient. On the right side, there is a complex network diagram consisting of numerous light blue dots connected by thin, light blue lines, creating a web-like structure that extends from the top right towards the bottom right.

STATISTICS ON BOTNET-ASSISTED DDOS ATTACKS IN Q1 2015

CONTENTS

Methodology	3
Main findings	4
Geography of attacks	5
Time variations in the number of DDoS attacks	7
Types and duration of DDoS attacks	9
C&C servers and botnet types	10
Conclusion	11
Glossary	12

METHODOLOGY

A DDoS (Distributed Denial of Service) attack is one of the techniques mostly often used by cybercriminals. It is intended to reduce an information system, typically a website, to a state where it cannot be accessed by legitimate users. One popular DDoS scenario is a botnet-assisted attack.

Kaspersky Lab has long-standing, recognized expertise in combatting cyberthreats, including DDoS attacks of different types and varying degrees of complexity. The company's experts, in particular, monitor botnet activity with the help of the DDoS Intelligence system (a part of [Kaspersky DDoS Protection](#) solution), which allows them to continuously improve our DDoS attack protection technologies. The DDoS Intelligence system is based on analyzing commands that arrive to botnets from C&C servers; it does not require a bot to be present on a user device, nor commands from the C&C server to be executed.

There are different approaches to analyzing DDoS activity. One of these is to focus on attacks against specific web resources, typically those belonging to clients protected against DDoS attacks by security service providers. However, the analysis of botnet activity in this report provides a different view of this problem, compared to the individual client-based approach.

This report presents DDoS Intelligence statistics collected from 1 January to 31 March 2015 (or Q1 2015), which is analyzed in comparison with the equivalent data collected within the previous 3-month period (1 October to 31 December 2014, or Q4 2014). In this report, a single DDoS attack is defined as an incident during which there was no break in botnet activity lasting longer than 24 hours. Thus, if the same web resource was attacked by the same botnet after a 24-hour gap that would be regarded as two separated DDoS attacks. Attacks on the same web resource from two different botnets are also regarded as individual attacks.

The geographical distribution of DDoS victims and command & control servers is determined according to their IP addresses. In this report, the number of the unique DDoS targets is defined 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 borne in mind that botnets are only one of the tools for carrying out DDoS attacks; thus, the data presented in this report does not cover every last DDoS attack that has occurred within the specified time period.

MAIN FINDINGS

- In Q1 2015, 23,095 botnet-assisted DDoS attacks were reported, which is 11% lower than the 25,929 attacks in Q4 2014.
- There were 12,281 unique victims of DDoS attacks in Q1 2015, which is 8% lower than the 13,312 victims in Q4 2014.
- China, the USA and Canada were the countries that faced the largest number of DDoS attacks.
- The most prolonged DDoS attack in Q1 2015 lasted for 140 hours (or about 6 days). The most frequently attacked resource faced 21 attacks within the 3 months.
- In Q1 2015, SYN DDoS and HTTP DDoS were the most common scenarios for botnet-assisted DDoS attacks.

GEOGRAPHY OF ATTACKS

In Q1 2015, 23,095 DDoS attacks were reported, targeting web resources in 76 countries. The number of attacks was down 11% against Q4 2014 (25,929). There was an increase (76 against 66 in Q4 2014) in the number of countries where DDoS targets were located.

Most DDoS attacks targeted web resources in China, the USA and Canada – this was no change from Q4 2014. There were some changes in the order of the 10 most frequently attacked countries, but there were no new additions to that list.

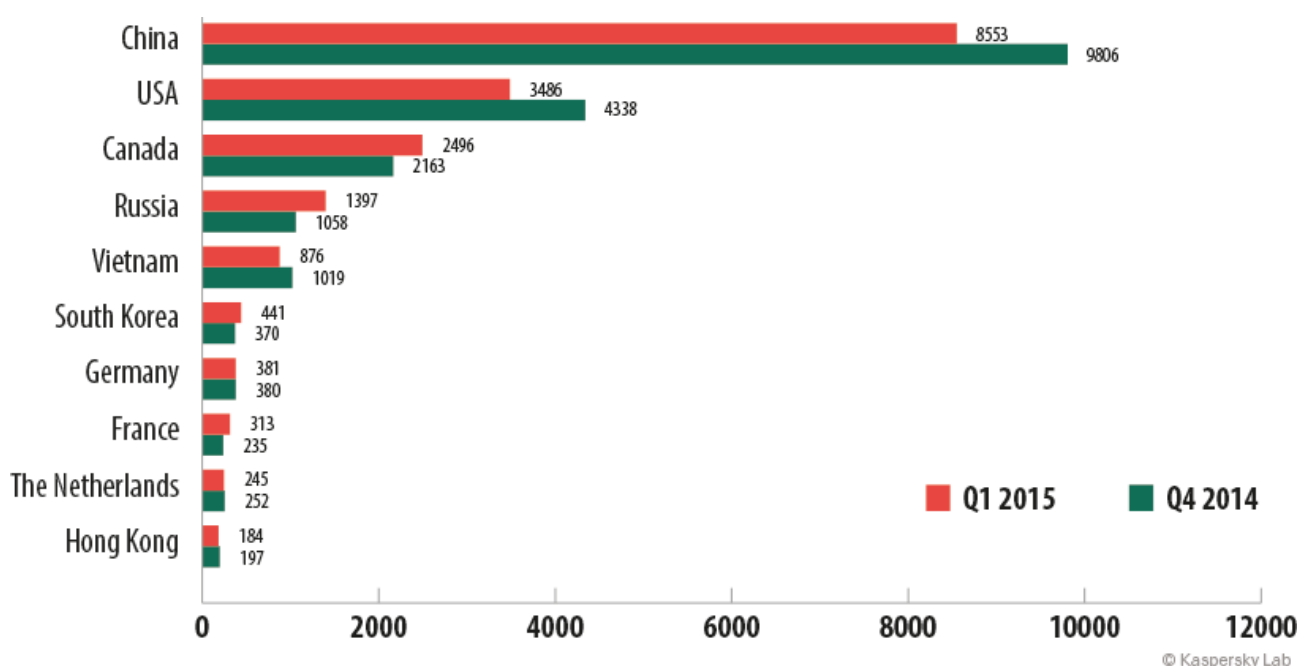


Figure 1. The 10 most frequently attacked countries in Q4 2014 and Q1 2015

As seen in the above diagram, there has been a significant decrease in the number of attacks against the web resources in China and the United States of America; however, there was an increase in the number of attacks against Canadian servers. There was also an increase in the number of attacks against web resources in Russia, South Korea and France.

If we consider the number of DDoS attack victims in each country, the top 10 looks the same as the previous one. In Q1 2015, botnets attacked a total of 12,281 victims, which is 8% lower than the 13,312 targets in Q4 2014.

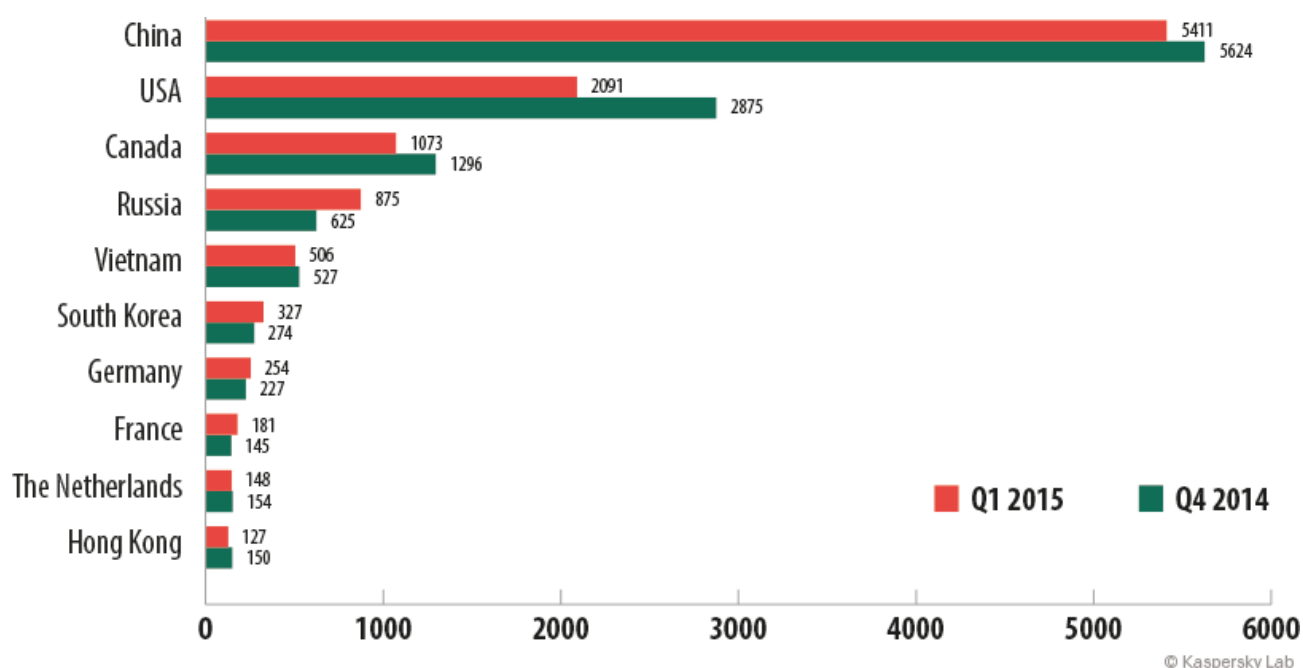


Figure 2. TOP 10 countries with the highest numbers of unique DDoS victims in Q4 2014 and Q1 2015

In Russia, South Korea and France, the number of attacked web resources has increased compared with Q4 2014, and so did the number of attacks on all targets located in these countries. In Canada, the number of attacks has increased, but the number of targets has decreased, which suggests that cybercriminals are more actively attacking a limited number of web resources in the country.

The fact that China and the USA lead the two rankings, both in terms of numbers of DDoS attacks and in numbers of victims, is explained by the relatively low web hosting prices in these two countries that encourage many companies to use hosting providers there.

In Q1 2015, the maximum number of attacks carried out on the same web resource reached 21:

Number of DDoS attacks	The targeted web resource
21	A Russian-language web-site (a group of investment companies)
16	A Vietnamese web-site (wedding services provider)
15	A hosting provider in the USA

Figure 3. TOP 3 most frequently attacked web resources in Q1 2015

Although China, the USA and Canada sustained the highest number of DDoS attacks in Q1 2015, the top two most frequently attacked web resources were respectively a Russian and a Vietnamese web-site. Only one of the top three, a US hosting provider, is based in the most frequently attacked trio of countries.

TIME VARIATIONS IN THE NUMBER OF DDoS ATTACKS

In Q1 2015, there were substantial time variations in the numbers of DDoS attacks¹. In late January there was a peak in botnet activity and the low point came in mid-February.

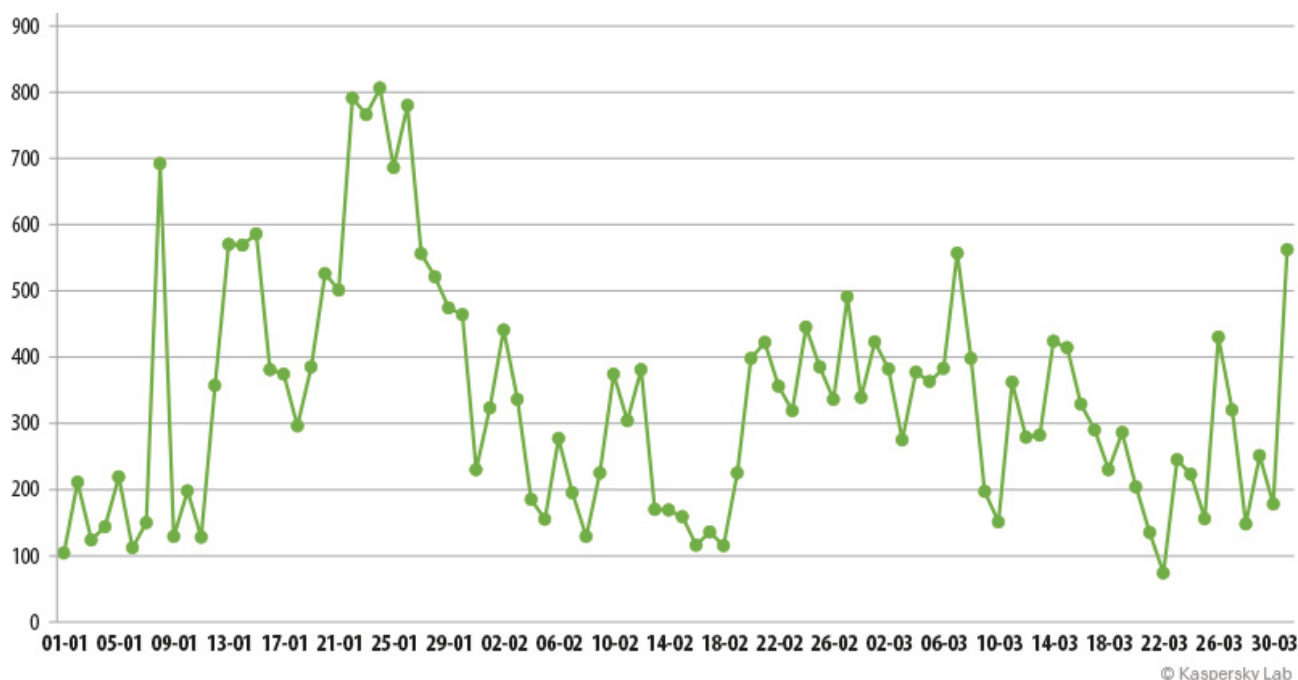


Figure 4. Number of DDoS attacks over time in Q1 2015

As seen in the chart below, last December saw a dramatic increase in the number of botnet-assisted DDoS attacks. The number of attacks declined steadily through January and February, but then began to rise again in March. The December peak could be linked to the Christmas / Near Year holidays, when the cybercriminals redoubled their efforts to disrupt the operation of websites and services popular with users.

¹ DDoS attacks may last for several days. In this graph, the same attack may be counted several times along the timeline, i.e. one time for each day of its duration. This results in a larger total number of DDoS attacks (30,064) than if each uninterrupted attack is counted as one (23,095).

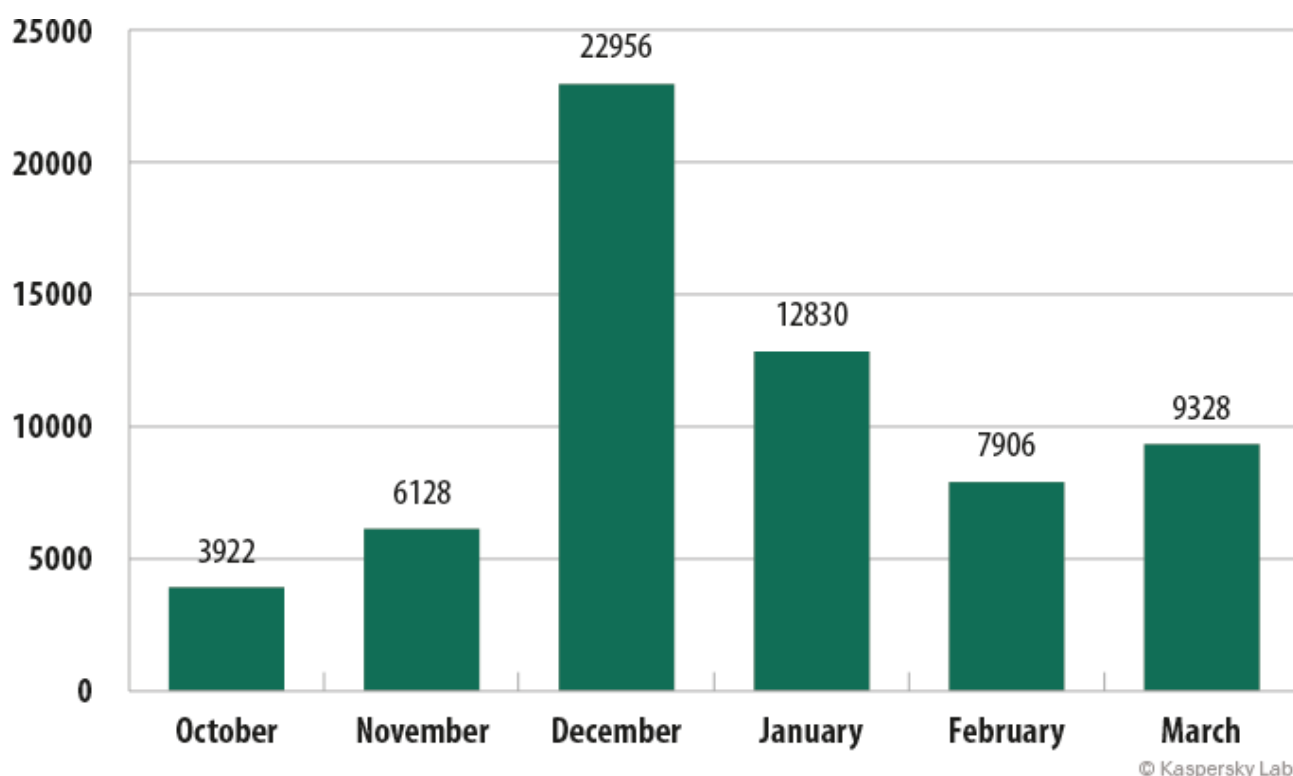


Figure 5. Monthly numbers of DDoS attacks in Q4 2014 and Q1 2015.

In Q1, Thursday became the most active day of the week in terms of numbers of botnet-assisted DDoS attacks, rather than Monday in Q4 2014. Sunday remains the quietest day for cybercriminals.

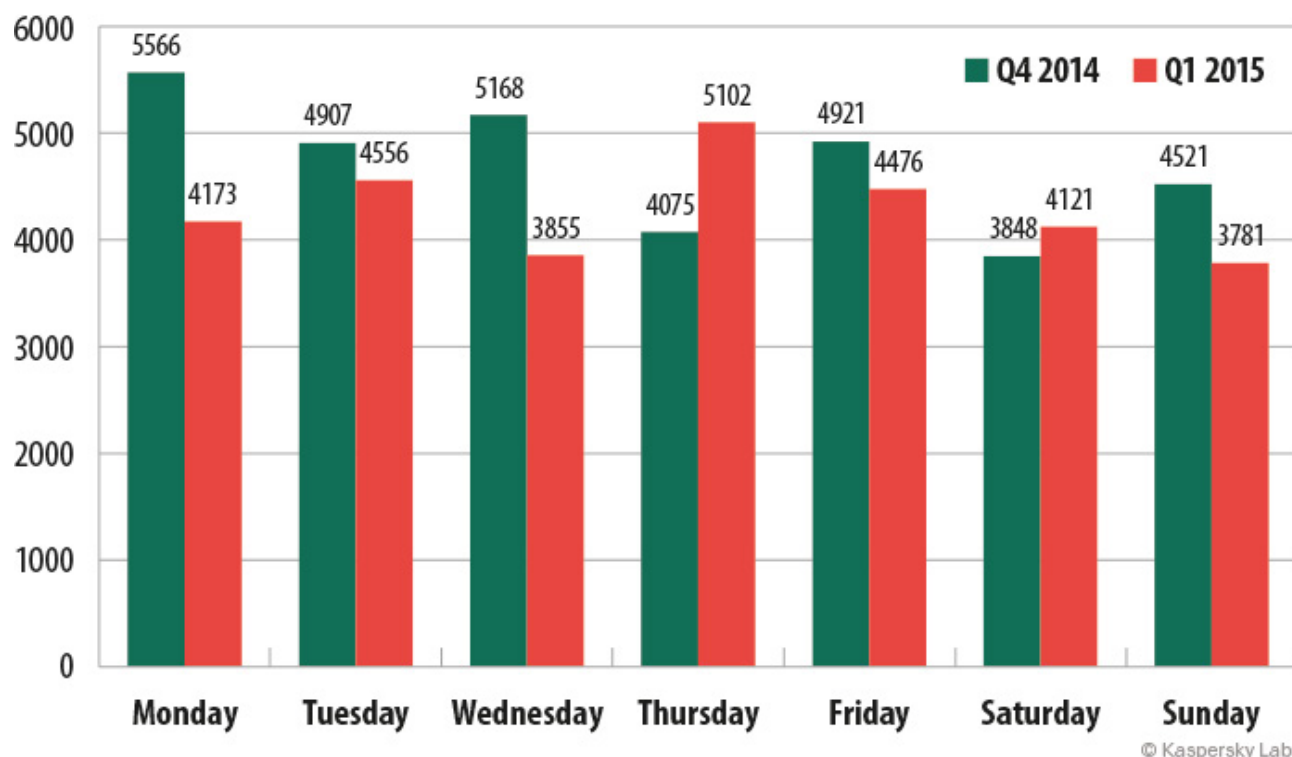


Figure 6. Numbers of DDoS attacks performed on each day of the week in Q4 2014 and Q1 2015

TYPES AND DURATION OF DDOS ATTACKS

The duration and the scenario of a DDoS attack are among its most important characteristics, as they define the extent of the damage inflicted on the target. Within the analyzed time period, the vast majority of attacks lasted less than 24 hours. In Q4 2014, some attacks lasted for up to two weeks; in Q1 2014, there were no attacks that would last this long.

Attack duration, hours	Number of targets in Q4 2014	Number of targets in Q1 2015
150+	5	0
100-149	8	3
50-99	299	121
20-49	735	433
10-19	1679	703
5-9	2161	1426
Less than 4	8425	9594

The type of a DDoS attack is defined by the format of junk requests sent to the target web resource. SYN DDoS was the most popular method of performing a DDoS attack in Q1 2015, just like in Q4 2014. TCP DDoS attacks were overtaken by HTTP DDoS attacks in second place.

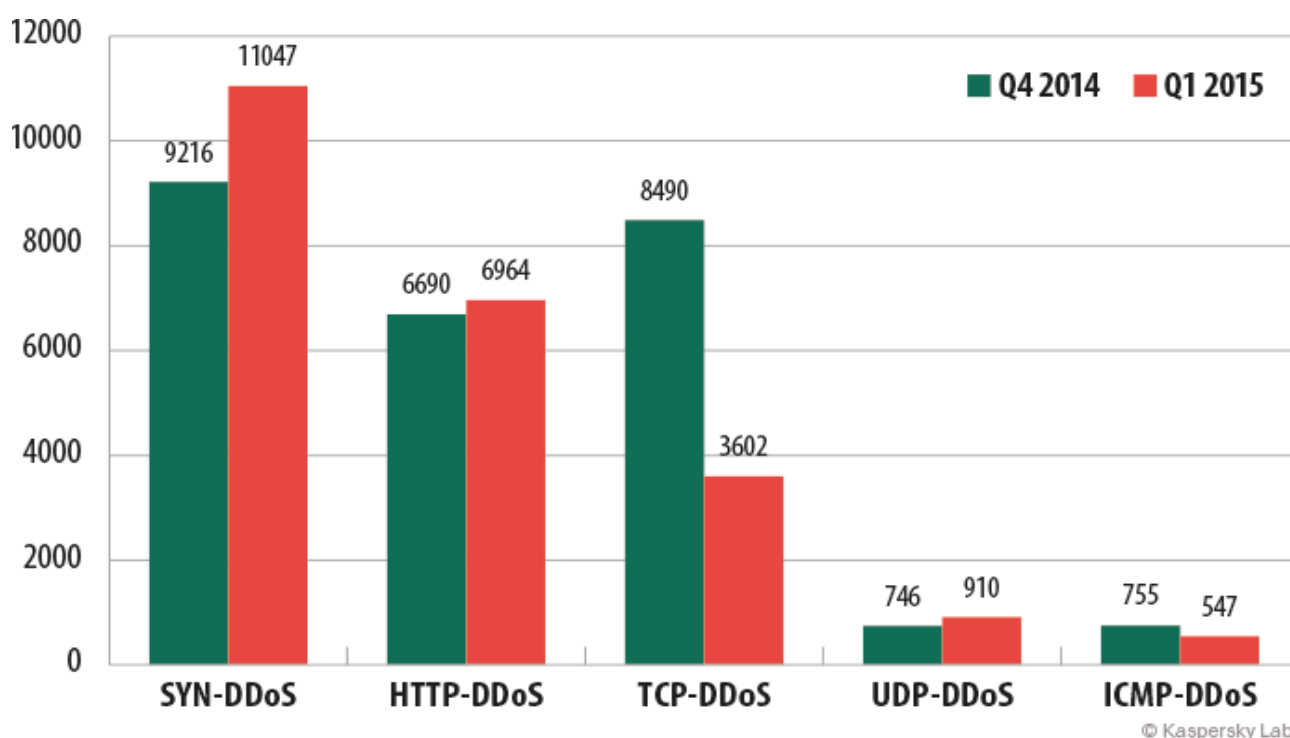


Figure 8. The most frequently used types of DDoS attacks in Q4 2014 and Q1 2015

C&C SERVERS AND BOTNET TYPES

The C&C servers used by cybercriminals to control botnets may be located in different countries. Their locations are not typically related to the cybercriminals' physical location(s) or to the geographic distributions of the botnets controlled via these C&C servers. The USA, China and the UK host the largest numbers of C&C servers that were active in Q1 2015.

In Q1 2015, just like in Q4 2014, bots designed to infect Linux servers were more active than those targeting Windows devices. At the same time, there was virtually no change in the number of attacks launched using Windows botnets, while the number of attacks from Linux botnets has decreased.

Although there are far fewer Linux-based botnets, the number of attacks launched from them is larger than that of the attacks launched from Windows-based botnets; also, the attacks from Linux-based botnets are more powerful. This is because a successful infection of a Linux-based server provides the cybercriminals with vast opportunities to manipulate network protocols. In addition, infected servers typically have faster internet connections than individual computers, so more powerful attacks can be carried out.

Besides, Linux-based botnets have much longer lives than Window-based botnets do. This is because Linux-based botnets are more difficult to detect and deactivate, since Linux servers are much less likely than Windows-based servers and devices to be equipped with dedicated security solutions.

It should be also pointed out that 93.2% DDoS targets in Q1 were attacked by just one family of bots. In 6.2% cases, two families of bots simultaneously participated in an attack, and three or more participated in 0.6% cases. In such cases, either the cybercriminals simultaneously used several different bot families to perform the attack, or the clients used the services of several attackers at once.

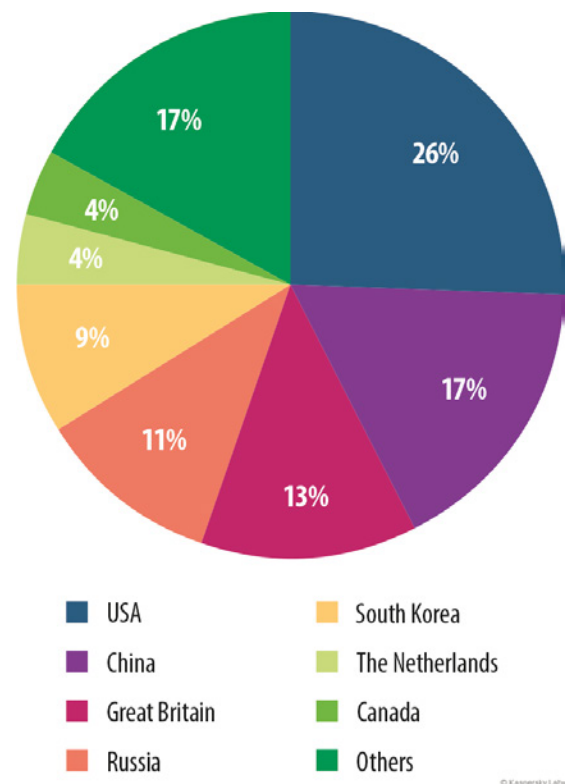


Figure 9. Numbers of botnet C&C servers by country, Q1 2015

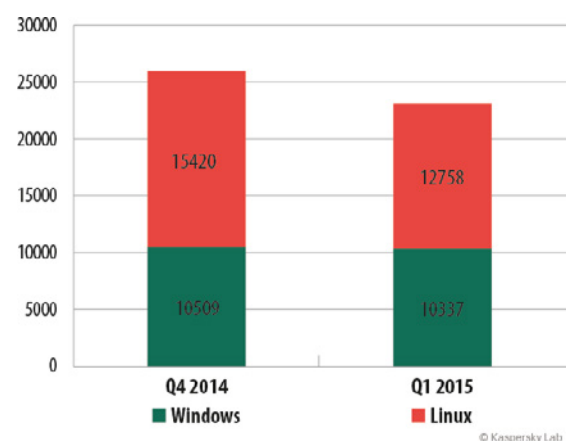


Figure 10. The number of attacks launched from Windows and Linux botnets in Q4 2014 and Q1 2015

CONCLUSION

The number of botnet-assisted DDoS attacks has declined in Q1 2015 against Q4 2014; so has the number victims of these attacks. At the same time, this type of threat has grown to target more countries. Historically, most attacks target web resources located in the USA and China, as these two countries offer the cheapest prices for web hosting, and many web resources are located there. However, the 10 most frequently attacked targets also include victims from Europe and the APAC region. These statistics demonstrate that botnet-assisted DDoS attacks are relevant for most diverse web resources irrespective of their geographic location. Moreover, this threat is increasingly expanding its boundaries.

The cybercriminals who use botnets to carry out DDoS attacks are willing to persevere: the longest DDoS attack reported in Q1 2015 lasted for about 6 days, and the most frequently attacked web resource survived 21 attacks within the three month period. However, study shows that even a short, one-off attack may render an unprotected web resource inoperable. One such attack may cost the victim up to [\\$444,000](#), not including the reputational damage associated with the unsatisfied users who failed to receive the service they expected.

Internet security companies make their contribution to combating DDoS attacks and botnets: among other things, they detect new pieces of malware and add signatures for them to the appropriate databases, protect servers from being compromised, protect computers against infections, [curb C&C server activities](#), etc. Nevertheless, DDoS attacks remain a very popular tool with cybercriminals, so companies must take proactive care of their security. A junk traffic filtration service will allow an online resource to remain accessible for legitimate users even during a long and powerful attack.

LINKS THAT MAY BE OF INTEREST:

[The botnet ecosystem](#)

[The economics of Botnets](#)

[IT Security Risks survey 2014: DDoS](#)

[Kaspersky DDoS Protection webpage](#)

[Kaspersky DDoS Protection whitepaper](#)

GLOSSARY

A bot is a malicious program that performs various actions at a cybercriminal's command.

A family of bots is an aggregate of bots sharing the same source code. In other words, these are different versions of the same bot, even if they are serviced by different C&C servers.

A botnet is an aggregate of devices infected with the same bot that is serviced by the same C&C server. Cybercriminals distribute special malicious programs which turn servers, computers or mobile devices into remotely managed 'zombies' (or bots).

A C&C (command and control) server is a server used by cybercriminals to send orders to bots and to receive reports from them. In the case of a DDoS attack, cybercriminals command bots to simultaneously send requests directly to the targeted web resource or via third-party servers, and thus carry out a 'distributed attack'.

SYN DDoS is an aggregate of DDoS attack scenarios which exploit peculiarities in the implementation of the TCP (Transmission Control Protocol). A TCP connection is established in three steps, which resembles the process of a handshake. The client sends a packet with the SYN flag. The server receives the SYN packet and replies with a packet with the headers SYN and ACK. Then the client sends an ACK packet, and thus validates the connection. In a SYN flood attack, the attacker sends packets with a SYN flag but does not require a response packet with SYN+ACK flags to establish a connection; this causes the targeted server to waste resources on processing these requests and sending response packets.

TCP DDoS is an aggregate of attack scenarios which, just like a SYN flood, exploit peculiarities in the implementation of the TCP protocol, but establish a connection to the targeted server. In a TCP flood-type attack, once the handshake procedure is completed successfully, the attacker side uses the established connection to send a lot of junk data, or send junk data in a very slow fashion. This overloads the attacked server, so it cannot allocate resources to legitimate users.


ICMP DDoS is an aggregate of attack scenarios using the ICMP (Internet Control Message Protocol). This protocol is normally used to send messages about errors or other exceptional situations that occur while transmitting data. In the case of an attack, the attacker sends plenty of ICMP requests to the victim side, forcing it to use its computational resources to process junk requests in place of legitimate requests.

UDP DDoS is an aggregate of attack scenarios that use UDP (User Datagram Protocol), which does not require a connection to be established. The attacker sends plenty of UDP packets to the victim's side. Each packet requires processing resources from the targeted server and its communication equipment; this overloads the victim's computational resources.


HTTP DDoS includes all types of DDoS attacks which have web applications as their target. While carrying out an attack, the attacker may send simple GET/POST requests to the main page of the web application as well as non-typical requests, such as requests to search for information in the web application's database, execute scripts on the web server side, etc. Extra headers or cookie files may be inserted in the request body; this is done to bypass the filters that determine a legitimate user by the presence of cookie files. Besides, the attacker may open the browser on an infected device in order to imitate the activities of a regular website visitor, and thus prevent the security systems on the victim side from detecting bots in the general visitor traffic.

 [Twitter.com/
KasperskyLabB2B](https://twitter.com/KasperskyLabB2B)

 [Facebook.com/
Kaspersky](https://facebook.com/Kaspersky)

 [Youtube.com/
Kaspersky](https://youtube.com/Kaspersky)

 [Linkedin.com/company/
kaspersky-lab](https://linkedin.com/company/kaspersky-lab)

 [Business.kaspersky.
com](https://business.kaspersky.com)

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

© 2015 Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners. Lotus and Domino are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Google is a registered trademark of Google, Inc.

