

Authorwww.securelist.com/en/analysis/204792189/DDoS_attacks_in_Q2_2011*Yury Namestnikov*

DDoS attacks in Q2 2011

All statistical data presented in this report were obtained using Kaspersky Lab's botnet monitoring system and Kaspersky DDoS Prevention.

The quarter in figures

- The most powerful attack repelled by Kaspersky DDoS Prevention in Q2: 500 Mbps
- The average power of the attacks repelled by Kaspersky DDoS Prevention: 70 Mbps
- The longest DDoS attack in Q2: 60 days, 1 hour, 21 minutes and 9 seconds
- The highest number of DDoS attacks against a single site in Q2: 218.

DDoS and protests

Distributed denial-of-service attacks are no longer being carried out simply to make a profit. Cybercriminals are increasingly targeting government resources or the sites of big companies to show off their skills, demonstrate their power or, in some cases, as a form of protest. These are exactly the sort of attacks that get maximum publicity in the media.

The most active hacker groups in the second quarter of 2011 were LulzSec and Anonymous. They organized DDoS attacks on government sites in the US, the UK, Spain, Turkey, Iran and several other countries. The hackers managed to temporarily bring down sites such as cia.gov (the US Central Intelligence Agency) and www.soca.gov.uk (the British Serious Organized Crime Agency (SOCA)). This shows that even government sites safeguarded by specialist agencies are not immune to DDoS attacks.

Attacking government sites is a risky business for hackers because it immediately attracts the attention of law enforcement authorities. In Q2 of 2011, for example, more than 30 members of Anonymous were arrested on suspicion of launching DDoS attacks on government sites. More arrests are likely to follow as authorities continue their investigations. However, not all those involved are likely to be convicted because participation in the organization of a DDoS attack is still not considered illegal in many countries.

One big corporation subjected to a major attack was Sony. At the end of March, Sony brought legal action against several hackers accusing them of breaching the firmware of the popular PlayStation 3 console. In protest at Sony's pursuit of the hackers, Anonymous launched a DDoS attack that crippled the company's PlayStationnetwork.com sites for some time. But this was just the tip of the iceberg. According to Sony, during the DDoS attack the servers of the PSN service were hacked and the data of 77 million users were stolen. Whether or not it was done intentionally, the DDoS

attack by Anonymous served as a **diversionary tactic** for the theft of huge volumes of data and which, at the end of the day, affected Sony's reputation.

DDoS attacks on social media

The second quarter of 2011 is likely to be remembered by Russian Internet users for the series of attacks on LiveJournal. The resource is popular with a variety of people, with housewives, photographers, pilots and even politicians posting blogs on the site. According to our botnet monitoring system, the mass attacks on LiveJournal began by targeting journals of a political nature, in particular, that of the anti-corruption and political activist Alexey Navalny.

Our botnet monitoring system has been tracking a botnet named Optima which was used in the DDoS attacks on LiveJournal. In the period between 23 March and 1 April Optima received commands to attack the anti-corruption site <http://rospil.info>, <http://www.rutoplivo.ru> and <http://navalny.livejournal.com> as well as the furniture factory site <http://www.kredo-m.ru>. On certain days only <http://navalny.livejournal.com> was attacked. At the beginning of April the botnet received a command to attack a long list of LiveJournal addresses mostly belonging to popular bloggers who cover a wide range of subjects.

The Optima botnet has been known on the market since late 2010. From the type of code used, it is safe to say that Optima bots are developed by Russian-speaking malware writers and they are mostly sold on Russian-language forums. It is difficult to determine the size of the botnet because it is highly segmented. However, our monitoring system has recorded instances of the Optima bots that attacked LiveJournal receiving commands to download other malicious programs. This suggests the Optima botnet includes tens of thousands of infected machines because such downloads are considered unprofitable for small botnets.

The motive for the attacks on LiveJournal remains unclear as nobody has yet claimed responsibility. Until the cybercriminals behind the attacks are identified, it will be difficult to say whether the attacks were ordered or just a show of force.

DDoS attacks on social media are becoming more frequent because these services allow the immediate exchange of information between tens of thousands of users. Blocking this process, even if it is just for a short time, can only be achieved with the help of DDoS attacks.

We expect to see a further growth in these types of attack in the future.

Commercial DDoS attacks

Ordinary criminals also continue to make active use of DDoS attacks. However, information about attacks that aim to extort or blackmail organizations is rarely made public and when it is, it is usually related to the subsequent criminal investigation.

In April, a court in Dusseldorf handed down a sentence to a cybercriminal who tried to blackmail six German bookmakers during the 2010 World Cup. The culprit used the familiar routine of: intimidation, a trial attack on the victim's site, and a message containing a ransom demand. Three of the six offices agreed to pay off the attacker. According to the bookmakers, a few hours of website downtime can result in the loss of significant sums – 25-40,000 euros for large offices and 5-6,000 euros for smaller offices. Surprisingly, the scammer only demanded 2000 euros. He received money in U-cash vouchers – a method which had already been used by the author of the well-known GpCode Trojan program. The court sentenced the defendant to nearly three years in

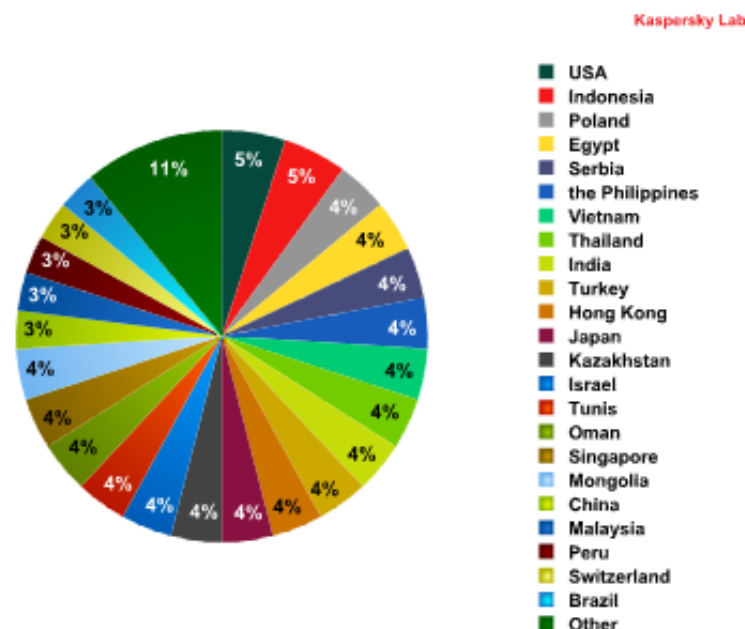
prison – the first time in German legal history that someone has been imprisoned for organizing a DDoS attack. Such attacks are now classified by the country's courts as computer sabotage and are punishable by up to 10 years in jail.

In June, the Russian judicial system also addressed the subject of DDoS attacks. On 24 June, a Moscow court sanctioned the arrest of Pavel Vrublevsky, the owner of ChronoPay, Russia's biggest Internet payment service provider. Vrublevsky was accused of organizing a DDoS attack against competitor firm Assist in order to undermine its chances in a tender for a lucrative contract to process payments for Aeroflot, Russia's largest airline. Sources close to the investigation said Vrublevsky was also considered the owner of the Rx-Promotion affiliate network which specializes in spreading pharmaceutical spam.

Statistical summary

Distribution of DDoS attacks by country

According to our statistics for Q2 2011, 89% of DDoS traffic was generated in 23 countries. The distribution of DDoS sources was fairly evenly spread among those countries, with each accounting for 3-5% of all DDoS traffic.



Distribution of DDoS attacks by country in Q2 2011

Most attacks came from the US and Indonesia with each country accounting for 5% of all DDoS traffic.

The US's leading position is down to the large number of computers in the country. Last year, US law enforcement authorities waged a successful anti-botnet campaign which led to the closure of a number of botnets. It is quite possible that cybercriminals will try to restore the lost botnet capacities and the number of DDoS attacks will increase.

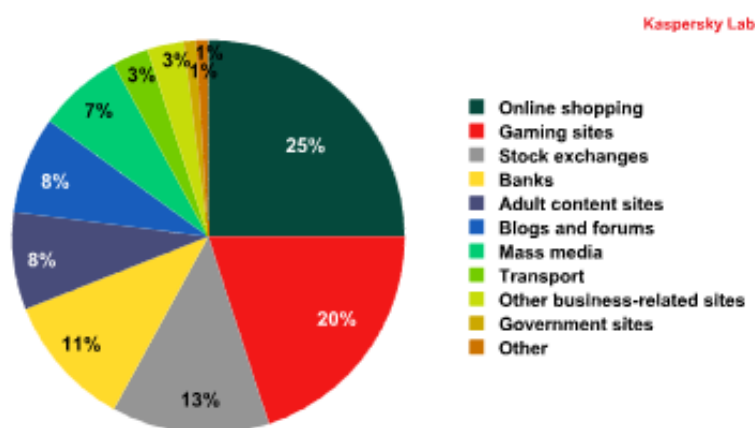
Meanwhile, the large number of infected computers in Indonesia means it also ranks highly in the DDoS traffic rating. In Q2 of 2011, almost every second machine (48%) on the Indonesian segment of Kaspersky Security Network, Kaspersky Lab's globally-distributed threat monitoring network, was subjected to a local malware infection attempt. Such a high percentage of blocked local infection

attempts is the result of a large number of unprotected computers being used to spread malware.

Those countries responsible for less than 3% of all DDoS traffic included countries with high levels of computerization and IT security (Japan, Hong Kong, Singapore) as well as countries where the number of computers per person is significantly lower and antivirus protection is far from perfect (India, Vietnam, Oman, Egypt, the Philippines, etc.).

Distribution of attacked websites by online activity

In Q2, online trading sites, including e-stores, auctions, buy and sell message boards etc., were increasingly targeted by cybercriminals – websites of this category accounted for a quarter of all attacks. This is hardly surprising: online trading largely depends on a website’s availability, and each hour of downtime results in lost clients and lost profits. This explains why these types of sites were targeted most often – competitors or straightforward extortion were usually behind the attacks.



Breakdown of attacked sites by areas of activity. Q2 2011

Gaming-related sites were the second most popular targets. As Kaspersky Lab’s monitoring system indicates, most attacks targeted EVE Online and its related websites. The MMORPG space-themed game had 357,000 active gamers as of late 2010. One site in particular that publishes EVE Online news experienced one of the most prolonged attacks – DDoS bots targeted it for 35 days. WoW and Lineage were also subject to some unwanted cybercriminal attention, although it was the games’ various pirate servers that suffered most.

The websites of electronic stock exchanges and banks occupy third and fourth places respectively. Cybercriminals attack trading platforms in order to cover their tracks after fraudulent transactions rather than to extort money. Typically, both the financial organizations and their clients lose money when such operations are performed. Therefore, how robust a service is against DDoS attacks is a factor that directly affects its reputation.

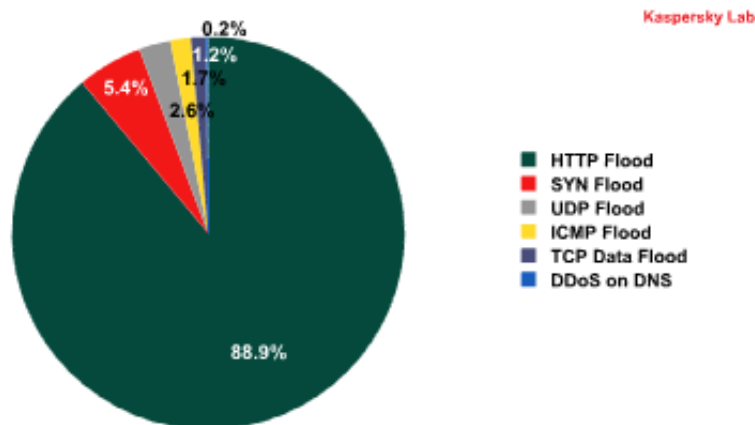
Interestingly, quite a substantial proportion of DDoS attacks targeted mass media sites (7%), and blogs and forums (8%), which are essentially a form of social mass media. We have already discussed the attacks on LiveJournal above. There is always someone who disagrees with a freely expressed opinion and it appears DDoS attacks are now being used as a means to silence media channels.

Governmental sites make up 1% of all attacked websites, although this statistic does not include attacks carried out by the group Anonymous using the “voluntary” botnet based on LOIC, a program used to arrange attacks. DDoS attacks are increasingly being used to lead protests against

government agencies in many countries, and we can expect to see more similar attacks in the future, especially at crucial stages in the political processes of societies.

Types of DDoS attacks

In Q2, Kaspersky Lab's botnet monitoring system intercepted over 20,000 web-borne commands to initiate attacks on different sites.



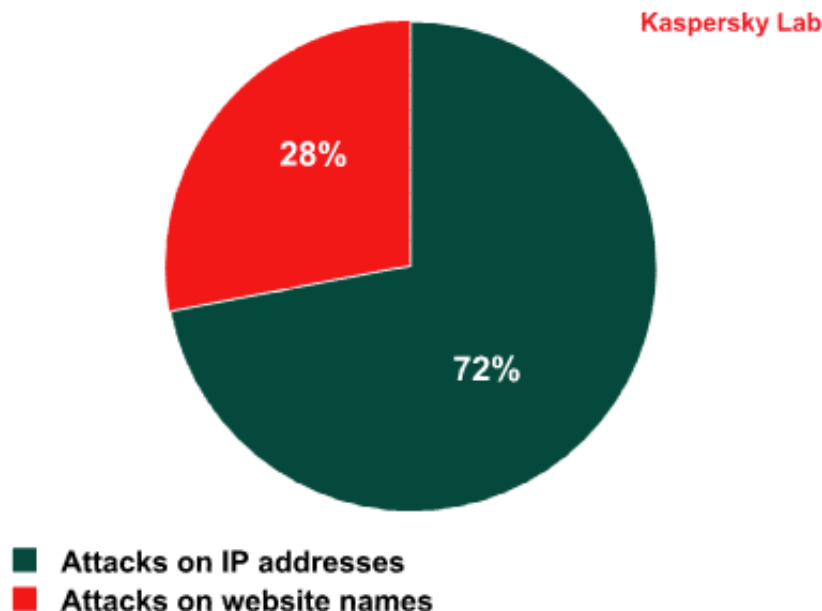
Types of DDoS attacks. Q2 2011

HTTP flood is the most popular (88.9%) method of attacking a website: a huge number of HTTP requests are sent to the targeted site over a short period. In most cases they look just like regular user requests, making it difficult to filter them out. This makes this type of DDoS attack more popular among cybercriminals than others.

SYN Flood attacks are the second most popular type of attack (5.4%). During such attacks, botnets send multiple data packages to the web server in order to establish a TCP connection. Cybercriminals manipulate packages so the server connections are left half open rather than established. Since a server can only maintain a limited number of connections at any time and botnets can generate lots of requests in short periods of time, the targeted server soon becomes unable to accept connections from regular users.

DDoS attacks on DNS servers (0.2%) were the least popular type of attack. As a result of this kind of attack DNS servers are unable to convert site names into IP addresses, so the sites serviced by the targeted server become unavailable to users. This type of attack is particularly damaging in that a single attack can render hundreds or even thousands of websites unavailable.

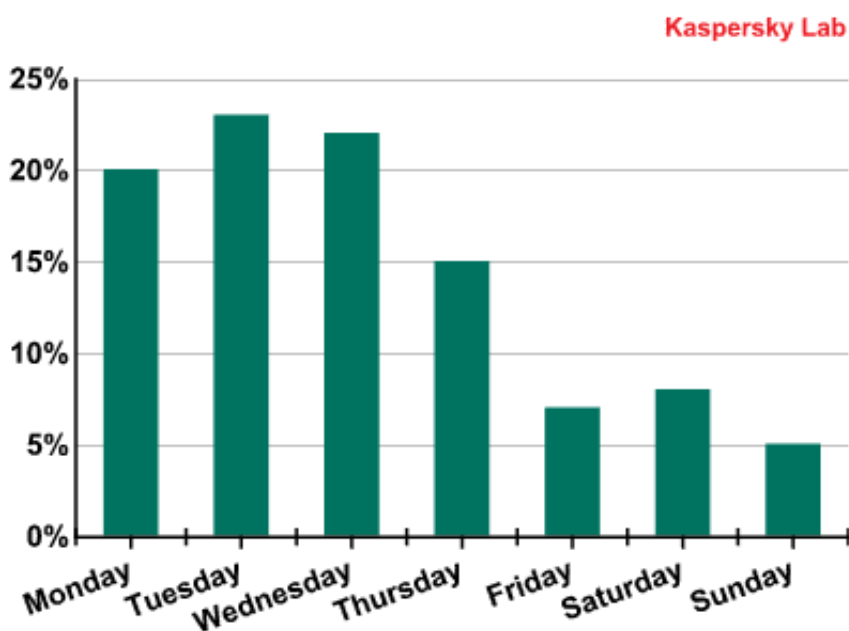
During a DDoS attack on one web resource, the bots received commands to send requests to an average of two web pages on the targeted site. If we compare the number of attacks delivered on site names and those on IP addresses, it can be seen that it is mostly IP addresses that are attacked: 72% of all attacks targeted IP addresses.



Breakdown of DDoS attacks by targets: site names vs. IP addresses. Q2 2011

Activity of DDoS botnets over time

Having analyzed all the available data, we can say on which days of the week cybercriminals prefer to carry out their attacks to bring down a site.



Breakdown of DDoS attacks by days of the week. Q2 2011

Weekdays see the most active use of the Internet. It is on these days that various web resources are most in demand and that DDoS attacks are likely to inflict the maximum amount of damage on websites. Another important factor is that greater numbers of computers are switched on on weekdays, so there are more active bots. As a result, cybercriminal activity peaks from Monday to Thursday – on these days an average of 80% of all DDoS attacks take place.

Conclusion

DDoS attacks have long been used for criminal purposes, but recently they have increasingly been used as a form of protest against the activities of both governments and major corporations. Such attacks receive widespread publicity in the mass media and are usually the subject of investigations by law enforcement agencies. We can expect to see the sites of government bodies in various countries increasingly come under attack as DDoS-based protests gain in popularity.

This does not mean that DDoS attacks are no longer used for extortion and blackmail. The victims, however, rarely acknowledge such incidents in order to protect their reputation. Cybercriminals are also increasingly using DDoS attacks as a diversionary tactic when launching more sophisticated attacks such as those on online banking systems. Complex attacks of this nature are particularly damaging in that they can cause significant losses for the financial institutions as well as their clients.

Most of the websites that we encounter as a result of DDoS attacks require much stronger protection. This is especially true as the summer holiday season comes to an end and more computers are switched on again, including zombie machines controlled by botmasters that will only make DDoS attacks more powerful and damaging.

© 1997-2011 Kaspersky Lab ZAO. All Rights Reserved.

Industry-leading Antivirus Software.

Registered trademarks and service marks are the property of their respective owners.

