

DOCUMENT* PRESENTED
BY WICK HILL

access
access
management
management
performance
performance
security
security
Convergence
Convergence

Wick Hill plc, River Court, Albert Drive, Woking, Surrey, GU21 5RP
01483 227600 | www.wickhill.com | info@wickhill.com

* © Wick Hill and the Wick Hill logo are trademarks of Wick Hill Group Plc. Registered in the UK and other countries. Other logo, brand and product names are trademarks of their respective owners. All 3rd party information contained within this document is copyright of the originator. Errors and omissions excluded.



Subject: Almost a quarter of all DDoS attacks fall on Tuesdays

Please see below the latest findings from Kaspersky Lab's analysis on DDoS attacks in Q2 2011.

Distributed denial-of-service attacks have long been used by cybercriminals resorting to blackmail and extortion. However, DDoS attacks are increasingly being used as a form of protest against the activities of both governments and major corporations. The second quarter of 2011 saw numerous DDoS attacks with a variety of motives, many of them significant enough to ensure they go down in the history of cybercrime, according to Kaspersky Lab.

The quarter in figures

- The longest DDoS attack in Q2 lasted 60 days, 1 hour, 21 minutes and 9 seconds
- The highest number of DDoS attacks against a single site in Q2: 218

Activity of DDoS botnets over time

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. The most popular day is Tuesday with roughly 23% of the week's DDoS attacks.

Distribution of attacked websites by online activity

In Q2 this year, online shopping sites, including e-stores, auctions, and buy and sell message boards, were increasingly targeted by cybercriminals – websites of this category accounted for a quarter of all attacks. This is hardly surprising: online shopping largely depends on a website's availability, and each hour of downtime results in lost clients and lost profits. The websites of electronic trading platforms and banks occupy third and fourth places respectively.

Q2 highlights

The most active hacker groups in the second quarter of 2011 were LulzSec and Anonymous. They organised 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 Organised Crime Agency (SOCA)).

One big corporation subjected to a major attack was Sony. At the end of March, Sony initiated 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.

“Organisations rarely publicise the fact that they have been targeted by DDoS attacks in order to protect their reputation. Cybercriminals, meanwhile, are 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,” explains Yury Namestnikov, senior malware analyst, Global Research and Analysis Team, Kaspersky Lab.

More information is available in the full version of the article 'DDoS attacks in Q2 2011' by Yury Namestnikov at: www.securelist.com/en

-ENDS-

Kaspersky Lab Newsroom

Kaspersky Lab has launched a new online newsroom, Kaspersky Lab Newsroom Europe (<http://newsroom.kaspersky.eu/en>), for journalists throughout Europe. The newsroom is specifically designed to serve many of the media's most common requests, making it easier for journalists to find product and corporate information, facts and figures, editorial copy, images, videos and audio files, as well as details about the appropriate PR contacts.

About Kaspersky Lab

Kaspersky Lab is the largest antivirus company in Europe. It delivers some of the world's most immediate protection against IT security threats, including viruses, spyware, crimeware, hackers, phishing, and spam. The company is ranked among the world's top four vendors of security solutions for endpoint users. Kaspersky Lab products provide superior detection rates and one of the industry's fastest outbreak response times for home users, SMBs, large enterprises and the mobile computing environment. Kaspersky® technology is also used worldwide inside the products and services of the industry's leading IT security solution providers. Learn more at www.kaspersky.co.uk. For the latest on antivirus, anti-spyware, anti-spam and other IT security issues and trends, visit <http://www.securelist.com>.

Editorial contact:

Berkeley PR
Amy Stevens
kasperskylab@berkeleypr.co.uk
Telephone: 0118 909 0909
Fax: 0118 988 6911
1650 Arlington Business Park
RG7 4SA, Reading

Kaspersky Lab UK
Ruth Knowles
Ruth.Knowles@kasperskylab.co.uk
Telephone: 0871 789 1633
Fax: N/A
Milton Business Park
OX14 4RY, Oxford

© 2011 Kaspersky Lab. The information contained herein is subject to change without notice. The only warranties for Kaspersky Lab products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Kaspersky Lab shall not be liable for technical or editorial errors or omissions contained herein.