Contacts:
Michelle Spencer
McAfee, Inc.
+44 (0)1753 513200
michelle_spencer@mcafee.com

Lee Whitehill
Interel
+44 (0)207 592 3812
lee.whitehill@interelconsulting.co.uk

SURVEY SHOWS JUST 2% OF MPS, BUSINESS LEADERS AND JOURNALIST BELIEVE THERE IS CYBER THREAT TO THE LONDON 2012 OLYMPICS,

McAfee experts believe the threat is much higher given the record increase of malware identified

LONDON, UK – Sept. 13, 2011 -- McAfee today announced survey results which show a worrying lack of awareness amongst MPs, business leaders and journalists about the extent of the cyber threat facing the London 2012 Olympic Games.

When asked to rate the greatest threat to the games only 2% of respondents named cyber compared to almost half of all respondents who believed a threat was more likely to come from a terror attack or transport failure.

The survey findings suggest that there is a continuing failure to grasp the importance of the cyber threat despite the government categorising the possibility of cyber-attack a tier one threat in the National Security Strategy and warnings from the London Organising Committee of the London Games (LOCOG) that attacks are "inevitable". McAfee's own research released on August 3 has shown that the International Olympic Committee (IOC) has already been the subject of cyber-attacks along with the networks of 72 organisations, although this has not been confirmed by the IOC. [see Operation Shady RAT: http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat].

Furthermore, Atos Origin, LOCOG's IT partner, have said that 14 million malware events were recorded per day during the Beijing Olympics, 400 of which had the potential to impact on the games. Fortunately, all of them were blocked.

In the first three months of 2011, McAfee identified more than six million examples of malicious software, which far exceeds any records for a similar time period. There has also been a 76% increase on attacks on android phones. At the current rate of growth McAfee expects samples to reach 75 million by the year end.

The survey showed:

- 52% of business leaders, 64% of politicians and 62% of journalists feel it is unlikely that there will be a large scale cyber-attack during London 2012;

- 74% of business people, 79% of politicians and 80% of journalists believe that if an attack took place it would not compromise the Games;
- 41% of respondents rated transport as the greatest threat to the success of the Games followed by 38% who rated terror attack as the biggest potential threat;
- Only 2% considered cyber-attack the largest threat which was less than those who thought lack of interest from the British public posed a greater problem.

However

- 89% of business leaders, 79% of MPs and 83% of journalists felt that the risk of cyber-attack will grow in the future.

David Blunkett, former Home Secretary and Chair of the International Cyber Security Protection Alliance (ICSPA) has called for an education campaign targeted at all parts of society. "At a time when cyber attacks on organisations like the IMF are hitting the headlines, it is important that our lawmakers and opinion formers understand the importance of the work being done to protect the London Olympic Games and use it as a springboard for a national campaign of online vigilance," he said.

The results are published as the House of Commons Science and Technology Committee announces that it will conduct a major inquiry into malware and cyber-attacks.

The YouGovStone survey commissioned by McAfee was carried out between 17 June and 12 July 2011, when a series of successful, high-profile cyber-attacks were being reported on the International Monetary Fund (IMF), the Pentagon and United States Senate. The hacking of millions of private files of millions of Nintendo and Sony games users were also being reported at this time, while according to the Government's Counter Terrorism Strategy, extremists called for a 'cyber-jihad' following the death of Osama Bin Laden.

When pressed respondents were able to demonstrate high level awareness among respondents of what comprises a cyber-attack which demonstrates a disparity between people's knowledge of what constitutes a threat and the vulnerability of major public spectacles such as the Olympics to cyber terrorist attacks.

When asked what areas were vulnerable to cyber threat, respondents said:

- Critical national infrastructure (74%-80%),
- Information systems (62% -73%),
- Computer viruses (31%-45%),
- PC hacking (35%-38%),

- State on state attacks (35%-39%),
- Identity theft (18%-23%).

Subsequently, when asked to consider what aspect of Olympic IT functions were most at threat, respondents rated transport infrastructure followed by an overall systems failure, co-ordination between Olympic venues, attacks on media, risk to personal details of competitors and teams, failure of timing systems and ticket sales to the public.

Rene Roersma, director of Global Public Sector, McAfee EMEA, said: “The organisers of the London Olympic Games and those in Government tackling the cyber issue are doing a tremendous job. However, the fact remains that 8,600 new crime Web sites are detected each day and a further 75 million new pieces of cybercrime software will be generated by the end of 2011.”

“The raising of the cyber threat to tier 1 status within the National Security Strategy and George Osborne’s comments at Google Zeitgeist conference that government is subject to 20,000 attacks each month, show that the issue is being addressed. The way forward is for civil government of all nations and defence organisations, including NATO, to continue working together alongside industry to safeguard, not just the Olympics, but also our critical infrastructure, commerce and national security,” continued Roersma.

-ENDS-

Notes to editors:

- McAfee is not associated with the London Olympics, the Olympics movement, the IOC or LOCOG and the LOCOG did not commission and have not commented on the survey. All comments cited in the press release were made by the individuals quoted.
- All figures, unless otherwise stated, are from YouGovStone Ltd. Total sample size was 300 individuals (100 business, 100 journalists, 100 MPs). Fieldwork was undertaken between June 17 and July 12, 2011. Survey results for MPs are representative of the House of Commons by Party, region and length of service.
- David Blunkett was appointed Chair of ICSPA in September 2010. The International Cyber Security Protection Alliance (ICSPA) is a global not-for-profit organisation established to channel funding, expertise and assistance directly to assist law enforcement cyber-crime units in both domestic and international markets.
- In the first three months of 2011, McAfee Labs identified more than six million unique malware examples which far exceed any records for a similar time period. At the current rate of growth, McAfee Labs expects samples to reach 75 million by the year end.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse and shop the Web more securely. Backed by its unrivalled Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. http://www.mcafee.com