McAfee AVERT Labs Celebrates 10 Years of Threat Protection and Predicts the Top Threats for 2006

2006 to See Dramatic Increase in Mobile Threats, While Phishing Scams and Identity Theft Will Continue to Rise

SANTA CLARA, Calif., Dec. 19 /PRNewswire-FirstCall/ -- McAfee, Inc.(NYSE: MFE), the leader in Intrusion Prevention and Risk Management solutions, today celebrates the tenth anniversary of McAfee(R) AVERT(R) Labs and its decade of tracking and providing protection against Internet threats. In conjunction with the anniversary, McAfee AVERT Labs also unveiled its outlook for security threats in 2006. The threat activity forecast includes an increase in mobile threats and the continued rise of phishing scams and identity theft.

Over the past ten years, McAfee AVERT Labs has seen the types and speed of threats change dramatically; from floppy disks, which spread through manual insertion of the disk into one computer after another, to more sophisticated techniques including mass-mailing threats, which still exist in numbers today, to threats that replicate effortlessly across networks and the globe via the Internet. According to McAfee AVERT Labs, there are now more than 160,000 various types of threats on the Internet today, and thousands more that have not yet been identified. These are all potential dangers to home and business computer users around the world.

In the ten years since McAfee AVERT Labs was established, the research laboratory has grown from a small team at McAfee headquarters in Santa Clara, Amsterdam, Paris and Sydney, to a globally distributed team with researchers and engineers in 20 cities, on five continents and in fourteen countries, 24 hours a day, seven days a week, 365 days a year.

McAfee AVERT Labs' experience and expertise was directly responsible for its discovery of two of the world's most high profile outbreaks - 'Melissa'in 1999 and 'MyDoom' in 2004. Jimmy Kuo, McAfee research fellow, not only named Melissa, but was instrumental in bringing the virus writer hunt to an end. Jimmy Kuo received a Fed 100 Award for his participation in and around the virus outbreak. He teamed with the government to successfully inform agencies about the threat and reduce the damage from the Melissa Virus. According to Computer Economics, the financial impact of Melissa in 1999 was estimated at 1.50 billion USD.

Craig Schmugar, researcher with McAfee AVERT Labs, was responsible for discovering MyDoom. The MyDoom worm gained the distinction of being the fastest spreading Malware attack ever, and according to Computer Economics, reached 12,000 systems per hour at its peak. The financial impact of MyDoom in 2004 was estimated at 5.25 billion USD.

McAfee AVERT Labs' 2006 Threat Forecast:

More Mobile Attacks -- A Serious Cause for Concern: Mobile malware was first sighted in June 2004 when a group of professional virus writers created the first proof-of-concept virus for smartphones -- demonstrating that malicious code could be created for Symbian operating systems. Soon after,'Duts' was released -- the first virus for Pocket PC Systems and the first file infector for smartphones. Since then, several mobile Trojans have appeared, resulting in an alarming growth of mobile malware.

McAfee AVERT Labs expects to see a significant rise in the number of global mobile threats in 2006. The use of smartphone technology has played a pivotal role in the threat's transition from multifunction, semi-stationary PCs to palm-sized "wearable" devices. And as a result of the increased connectivity of smartphones, McAfee AVERT Labs expects these threats to make a quick transition to converged devices.

McAfee AVERT Labs predicts that the damage caused by new mobile threats is likely to be more extensive than those caused by today's PC threats because of the large volume of smartphones and the small percentage that are protected by mobile security. For example, in 2004, the 'I Love You' virus penetrated tens of millions of PCs in just a couple of hours despite the fact that half of all PCs had Internet security software installed. By comparison, a mobile threat targeting several operating systems could infect up to 200 million connected smartphones simultaneously because the majority of these devices do not currently have mobile security protection installed.

According to McAfee AVERT Labs, since the inception of malware, mobile malware has grown almost 10 times faster than PC malware over a comparable period of one year.

Consumers are less likely to install mobile security versus PC security because the perceived risk from mobile threats is much less. However, creators of mobile malware have learned from PC hackers and virus writers to create sophisticated threats, invisible to the consumer, that provide them with financial gain. This will result in instantly mature mobile threats that can devastate networks and consumer data with little fanfare or warning.

PUPS Expected to Grow -- The Blurring of Boundaries: In 2005, McAfee AVERT Labs has seen a 40% increase in commercial Potentially Unwanted Programs (PUPs), and an even larger increase in related types of malicious Trojans, particularly keyloggers, password-stealers, bots and backdoors. In addition, misuse of commercial software by malware with remotely controlled deployment of adware, keyloggers and remote control software is on the rise.

While federal and state legislation moves forward at varying paces, industry groups like the AntiSpyware Coalition, of which McAfee is a founding member, have begun to define and categorize the problem of potentially unwanted behaviors. Likewise, efforts on the part of the advertising software industry at self-policing, such as 180Solutions suing rogue affiliates, have met with mixed success. Legal actions by adware vendors against anti-spyware vendors are increasing, as are enforcement actions by the Federal Trade Commission and the New York State Attorney General against adware vendors and affiliates. SonyBMG's use of rootkit technology in their copyright protections software further highlights the challenges of corporations and consumers in this shifting landscape. The new year will undoubtedly prove interesting.

Phishing and Identity Theft -- The Evolution of an Industry: Phishing first came to light as a major concern in 2004. Originally, phishing was a term used by hackers to describe stealing America Online(R) (AOL) accounts by acquiring usernames and passwords. Since then, the ability of criminals to take advantage of technology has increased significantly.

Phishing scams will continue to cause concern in 2006 as attacks become increasingly more targeted through the use of spyware programs and password stealers. Flaws in email protocols, security weaknesses in browser software,and a lack of basic computer security education will contribute to this increase in phishing incidents as criminals exploit these issues. McAfee AVERT Labs predicts an increase in distributed phishing Trojans -- Trojans that turn an infected computer into a phishing Web site and then spam others to go to that infected machine or site.

In 2006, McAfee AVERT Labs also expects to see a greater number of password stealing Web sites, more attacks that attempt to capture a user's ID and password by displaying a fake sign-in page, and increased targeting of popular online services such as eBay. As evidenced by the phishing attacks that followed Hurricane Katrina, McAfee AVERT Labs also expects more attacks that take advantage of people's willingness to help others in need. In contrast, the number of attacks on ISPs are expected to decline while those aimed at the financial sector will remain steady.

McAfee AVERT Labs' Recommendation

To protect against the above threats and malicious programs, McAfee AVERT Labs recommends both enterprises and consumers educate themselves about these threats and remain diligent by regularly updating to the latest DATs, installing the latest patches, employing current spam filters, and implementing a multi-layered approach to detecting and blocking attacks. For more information and solutions that can help enterprises and consumers ensure constant security protection, please visit www.mcafee.com.

About McAfee AVERT Labs

McAfee AVERT Labs maintains one of the top-ranked security threat and research organizations in the world, employing researchers in thirteen countries on five continents. The Labs combine world-class malicious code and anti-virus research with intrusion prevention and vulnerability research expertise from the McAfee IntruShield, McAfee Entercept, McAfee Foundstone Research and McAfee Foundstone Professional Services organizations. McAfee protects customers by providing deep analysis and core technologies that are developed through the combined efforts of its researchers.