Internet security systems report

Internet Security Systems(ISS), an IBM Company have releleased the highlights of its 2006 security statistics report, which describes key security findings for 2006 and predicts the nature of Internet threats expected to emerge in 2007. Based on early indicators, ISS anticipates a continued rise in the sophistication of profit-motivated cyber attacks, including an increased focus on the Web browser and advances in image-based spam. According to the report,, which was developed by the ISS X-Force research and development team, there were 7, 247 new vulnerabilities recorded and analysed by the X-Force in 2006, which equates to an average of 20 new vulnerabilities per day. This total represents a nearly 40 per cent increase over what ISS reported in 2005. Over 88 per cent of 2006 vulnerabilities could be exploited remotely, and over 50 per cent allowed attackers to gain access to a machine after exploitation.

> " While these numbers seem grim upon initial review, the good news is our research indicates a drop in the percentage of high-impact vulnerabilities since last year," - said ISS.

In 2005, high-impact vulnerabilities accounted for about 28 per cent of total vulnerabilities, while they only accounted for 18 per cent in 2006. The security industry has made great progress over the last year, but despite promising statistics such as this one, we predict that 2007 will require even higher levels of vigilance and innovation to deal with emerging threats and new vectors of attack. Attacks on Web browsers are expected to continue rising in 2007, partially as a result of the newly-created 'exploits as a service' industry. The sale of exploit material is becoming even more organised and is increasingly taking the shape of the channel sales model used by

legitimate corporate entities. Managed exploit providers are purchasing exploit code from the underground, encrypting it so that it cannot be pirated, and selling it for top dollar to spare distributors. The organised development and sale of encrypted exploit code will make signature-based protection even less effective in the new year. In terms of spam, X-Force predicts a continued sophistication of image-based spam techniques. In 2007, new forms of image-based spam will likely be developed to evade protection solutions that have been created to combat early forms of image-based spam seen in the wild.

This latest report from X-Force also points to new methods being used by attackers to avoid detection by commercial security solutions. In 2006, malware continued to become less distinct in its categorisation, instead borrowing characteristics from other successful forms of malware. As such, the classical groups of virus, rootkit, spyware and other categories typically used by the security industry to differentiate standalone protection products will be much less relevant in 2007.

In 2006, X-Force also observed considerable Web browser exploitation and a strong increase in the use of Web exploit obfuscation and encryption to make it difficult for signature-based intrusion detection and prevention products to detect attacks. X-Force data indicates that approximately 50 per cent of Web sites hosting exploit material designed to infect browsers now obfuscate or camouflage their attack, with approximately 30 per cent enerypting their payload. The X-Force has been cataloguing, analysing and researching vulnerability disclosures since 1997. With more than 30, 000 security vulnerabilities catalogued, it has the largest vulnerability database

in the world. This unique database helps X-Force researchers to understand the dynamics that make up vulnerability discovery and disclosure. In addition to the vulnerabilities catalogued in its X-Force database, ISS content filtering services are designed to provide a world-encompassing view of spam and phishing attacks. With millions of e-mail addresses actively monitored, ISS has identified numerous advances in the spain and phishing technologies used by online attackers.

During 2005 and 2006, X-Force data indicates that the use of image-based spam increased rapidly, accounting for more than 40 per cent of spam messages at the end of 2006. This issue quickly became one of the biggest challenges in spam-fighting for 2006 since it is difficult for spam blockers that rely on content identification to decode text embedded within images.

The X-Force report also discusses the following key security statistics for 2006, among others:

- Within the last year, the volume of spare has increased by 100 per cent over what ISS reported in 2005.
- The U. S., Spain and France are the three largest originators of spam worldwide.
- After English, German is the most popular language in which spare messages are written. (X-Force predicts that as computer users become more savvy at detecting and deleting spam, spammers will increasingly localise their messages in languages other than English to improve the rate at which they are opened.)
- The most popular subject line for spare in 2006 was 'Re: hi.'

- South Korea accounts for the highest source of phishing e-mails.
- The largest threat category of malware in 2006 was Downloaders, accounting for 22 per cent of all malware. (A Downloader is a piece of low-profile malware that installs itself on machines for the purpose of later downloading a more sophisticated malware agent.)
- The most popular exploit used on the Internet to infect Web browsers with malware was for Microsoft's MS-ITS vulnerability (MS04-013), disclosed in 2004.
- The busiest month in 2006 for vulnerability disclosure was June, while the busiest week was the week before Thanksgiving in November and the most popular day of the week to disclose vulnerabilities was Tuesday.

In 2007, ISS also expects to see a continued rise in the total number of vulnerabilities, largely due to the release of new operating systems. *While the new operating systems include more security functions than previous versions and have undergone extensive security audits, their sheer complexity will likely introduce new vulnerabilities* . In addition, the synchronised release of new and updated third-party products that support new operating systems will likely contribute to a record year for vulnerabilities in 2007.