New Internet Security Threat Research Reveals that Hackers are Adopting New Business-Like Strategies to Successfully Perform Malicious Activity

SYDNEY, Australia

–17 September 2007 – The latest Internet Security Threat Report (ISTR), Volume XII released today by Symantec Corp. (Nasdaq: SYMC) concludes that cyber criminals are increasingly becoming more professional – even commercial – in the development, distribution and use of malicious code and services. While cybercrime continues to be driven by financial gain, cyber criminals are now utilising more professional attack methods, tools and strategies to conduct malicious activity. www.symantec.com/threatreport/. Broadcast media can download multimedia at www.thenewsmarket.com/symantec. www.symantec.com/http://www.symantec.com/news. All prices noted are in U.S. dollars and are valid only in the United States. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

“As the global cyber threat continues to grow, it has never been more important to remain vigilant and informed on the evolving threat landscape,” said Dan Lohrmann, chief information security officer, State of Michigan. “Symantec's Internet Security Threat Report continues to provide us with critical information on the most current online security trends, helping us better protect our state’s infrastructure and citizen information.”

During the reporting period of Jan. 1, 2007, through June 30, 2007, Symantec detected an increase in cyber criminals leveraging sophisticated toolkits to carry out malicious attacks. One example of this strategy was MPack, a professionally developed toolkit sold in the underground economy. Once purchased, attackers could deploy MPack’s collection of software components to install malicious code on thousands of computers around the world and then monitor the success of the attack through various metrics on its online, password protected control and management console. MPack also exemplifies a coordinated attack, which Symantec reported as a growing trend in the previous volume of the ISTR where cyber criminals deploy a combination of malicious activity.

Phishing toolkits, which are a series of scripts that allow an attacker to automatically set up phishing Web sites that spoof legitimate Web sites, are also available for professional and commercial cybercrime. The top three most widely used phishing toolkits were responsible for 42 percent of all phishing attacks detected during the reporting period.

“In the last several Internet Security Threat Reports, Symantec discussed a significant shift in attackers motivated from fame to fortune,” said Arthur Wong, senior vice president, Symantec Security Response and Managed Services. “The Internet threats and malicious activity we are currently tracking demonstrate that hackers are taking this trend to the next level by making cybercrime their actual profession, and they are employing business-like practices to successfully accomplish this goal.”

Increase in Cyber Criminals Exploiting Trusted Environments to Target Victims

During the reporting period, Symantec detected attackers indirectly targeting victims by first exploiting vulnerabilities in trusted environments, such as popular financial, social networking and career recruitment Web sites. Symantec observed 61 percent of all vulnerabilities disclosed were in Web applications. Once a trusted Web site has been compromised, cyber criminals can use it as a source for distribution of malicious programs in order to then compromise individual computers. This attack method allows cyber criminals to wait for their victims to come to them verses actively seeking out targets. Social networking Web sites are particularly valuable to attackers since they provide access to a large number of people, many of whom trust the site and its security. These Web sites can also expose a lot of confidential user information that can then be used in attempts to conduct identity theft, online fraud or to provide access to other Web sites from which attackers can deploy further attacks.

Rise in Multi-Staged Attacks

During the first six months of 2007, Symantec observed an increase in the number of multi-staged attacks which consist of an initial attack that is not intended to perform malicious activities immediately, but that is used to deploy subsequent attacks. One example of a multi-staged attack is a staged downloader that allows an attacker to change the downloadable component to any type of threat that suits the attacker’s objectives. According to the ISTR, Symantec observed that 28 of the top 50 malicious code samples were staged downloaders. Peacomm Trojan, mostly known as Storm Worm, is a staged downloader that was also the most widely reported new malicious code family during the reporting period. In addition to serving as an attack toolkit, MPack is an example of a multi-staged attack that included a staged downloader component.

Additional Key Findings


* Credit cards were the most commonly advertised commodity on underground economy servers, making up 22 percent of all advertisements; bank accounts were in close second with 21 percent.
* Symantec documented 237 vulnerabilities in Web browser plug-ins. This is a significant increase over 74 in the second half of 2006, and 34 in the first half of 2006.
* Malicious code that attempted to steal account information for online games made up 5 percent of the top 50 malicious code samples by potential infection. Online gaming is becoming one of the most popular Internet activities and often features goods that can be purchased for real money, which provides a potential opportunity for attackers to benefit financially.
* Spam made up 61 percent of all monitored e-mail traffic, representing a slight increase over the last six months of 2006 when 59 percent of e-mail was classified as spam.
* Theft or loss of computer or other data-storage medium made up 46 percent of all data breaches that could lead to identity theft. Similarly, Symantec’s IT Risk Management Report found that 58 percent of enterprises expect a major data loss at least once every 5 years.

About the Symantec Internet Security Threat Report
The semiannual Symantec Internet Security Threat Report (ISTR), Volume XII covers the six-month period from January 1, 2007, through June 30, 2007. It is based on Symantec data collected from more than 40,000 sensors deployed in more than 180 countries in addition to a database that covers more than 22,000 vulnerabilities affecting more than 50,000 technologies from more than 8,000 vendors. Symantec also reviews more than 2 million decoy accounts that attract e-mail messages from 20 different countries around the world allowing Symantec to gauge global spam and phishing activity. The full Internet Security Threat Report includes additional statistics and detail and is available for download at

About Symantec
Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information and interactions by delivering software and services that address risks to security, availability, compliance and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at

###
NOTE TO EDITORS: If you would like additional information on Symantec Corporation and its products, please visit the Symantec News Room at

Media Contact:
Debbie Sassine
Symantec
+61 2 8879 1110
Debbie_sassine@symantec.com
Rachel York
Max Australia
+61 2 9954 3492
Rachel.york@maxaustralia.com.au