

Symantec Reports Rise in Data Theft, Data Leakage, and Targeted Attacks Leading to Hackers' Financial Gain

New Internet Security Threat Activity Research Reveals a Shift towards Collaborative, Global Online Communities Operated by Cyber Criminals

CUPERTINO, Calif. – March 19, 2007 – The latest Internet Security Threat Report released today by Symantec Corp. (Nasdaq: SYMC) reveals that the current Internet threat environment is characterized by an increase in data theft, data leakage, and the creation of targeted, malicious code for the purpose of stealing confidential information that can be used for financial gain. Cyber criminals continue to refine their attack methods in an attempt to remain undetected and to create global, cooperative networks to support the ongoing growth of criminal activity.

“Symantec’s Internet Security Threat Report gives our organization a detailed analysis of worldwide Internet threats, helping us monitor security risks and adjust our technology and protection processes accordingly,” said Dan Lohrmann, chief information security officer for the state of Michigan. “Safeguarding sensitive information and the public’s trust is essential for our support of Michigan agencies providing law enforcement, health care, and citizen service. The report’s comprehensive data on the global threat landscape complements our department’s security operations.”

Symantec’s Internet Security Threat Report Volume XI reveals:

- Symantec reported more than 6 million distinct bot-infected computers worldwide during the second half of 2006, representing a 29 percent increase from the previous period. However, the number of command-and-control servers used to relay commands to these bots decreased by 25 percent, indicating that bot network owners are consolidating their networks and increasing the size of their existing networks.
- Trojans constituted 45 percent of the top 50 malicious code samples, representing a 23 percent increase over the first six months of 2006. This significant increase supports Symantec’s forecast from previous research, which noted that attackers appeared to be making a shift away from mass-mailing worms toward using Trojans.
- Symantec documented 12 zero-day vulnerabilities during the second half of 2006, marking a significant increase from the one zero-day vulnerability documented in the first half of 2006, increasing the exposure of consumers and businesses to unknown threats.
- Underground Economy Servers are being used by criminals and criminal organizations to sell stolen information, including government-issued identity numbers, credit cards, bank cards and personal identification numbers (PINs), user accounts, and e-mail address lists.
- Theft or loss of a computer or data storage medium, such as a USB memory key, made up 54 percent of all identity theft-related data breaches.
- For the first time, Symantec identified the countries with the highest amount of malicious activity originating from their networks. The United States had the highest proportion of overall malicious activity, with 31 percent; China was second, with 10 percent; and Germany was third, with 7 percent.

“As cyber criminals become increasingly malicious, they continue to evolve their attack methods to become more complex and sophisticated in order to prevent detection,” said Arthur Wong, senior vice president, Symantec Security Response and Managed Services. “End users, whether consumers or enterprises, need to ensure proper security measures to prevent an attacker from gaining access to their confidential information, causing financial loss, harming valuable customers, or damaging their own reputation.”

Threats to Confidential Information on the Rise

For the first time, Symantec tracked the trade of stolen confidential information and captured data frequently sold on underground economy servers. These servers are often used by hackers and criminal organizations to sell stolen information, including social security numbers, credit cards, personal identification numbers (PINs), and e-mail address lists. During the last six months of 2006, 51 percent of all known underground economy servers in the world were located in the United States. U.S.-based credit cards with a card verification number were available for between US \$1 - \$6 while an identity, including a U.S. bank account, credit card, date of birth and government issued identification number, was available for between US \$14 - \$18.

During the reporting period, Symantec observed a rise in threats to confidential information due to the increase of Trojans and bot networks enabling an attacker to gain access to a victim’s computer. Attacks that obtain sensitive data stored on an infected computer can result in significant financial loss, particularly if credit card or banking information is exposed. Threats to confidential information made up 66 percent of the top 50 malicious code reported to Symantec, an increase over the 48 percent reported in the previous period. Threats that could export user data, such as user names and passwords, accounted for 62 percent of threats to confidential information during the second half of 2006, up from 38 percent in the first half of the year.

Increase in Data Breaches Help Facilitate Identity Theft

Confidential information used in identity theft is often confiscated as a result of a data breach. During the reporting period, Symantec assessed data breaches that resulted from hacker activity, the theft or loss of computer hardware, and security policy failure. Data breaches and the potential use of confidential information for identity theft can result in a loss of public confidence, legal liability, or costly litigation. The majority of global data breaches affected the government sector, accounting for 25 percent of the total. Government organizations may be considered a prime target as they often store data in many separate locations making it accessible to various people, and thereby increasing the opportunities for attackers to gain unauthorized access.

Rise in Sophisticated Spam and Online Fraud Schemes

Symantec observed high levels of coordinated attacks combining spam, malicious code, and online fraud. During the second half of 2006, spam made up 59 percent of all monitored e-mail traffic marking a steady increase over the first six months of 2006, with 30 percent of the total spam related to the financial services industry resulting from an increase in “pump-and-dump” spam. During a “pump-and-dump” scheme, cyber criminals profit by purchasing stock when it is low and then artificially pumping up interest in the stock by sending out spam containing false predictions of high performance for the stock. Spam recipients trust the content and buy the stock, creating demand and resulting in a rise in the stock price. When the stock price increases, the cyber criminals sell their stock for a profit.

Over the last six months of 2006, Symantec detected a total of 166,248 unique phishing messages, an average of 904 per day, marking a 6 percent increase over the first six months of 2006. For the first time, Symantec analyzed the effects that the day of the week and seasonal events may have had on phishing attacks. Throughout 2006, Symantec detected an average of 27 percent fewer unique phishing messages on weekends

than the average of 961 phishing messages on the weekdays. This trend indicates that phishing activity mirrors the business week where attackers attempt to mimic a legitimate company's e-mail practices. However, this pattern may also indicate that phishing campaigns are short lived and most effective when victims receive and read the phishing e-mails shortly after they were distributed. Symantec observed an increase in phishing activity during major holidays and other large events, such as the FIFA World Cup, due to the fact that attackers may find it easier to craft theme specific social engineering attacks surrounding special events.

About the Symantec Internet Security Threat Report

The semiannual Symantec Internet Security Threat Report (ISTR) Volume XI covers the six-month period from July 1, 2006, through December 31, 2006. 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 20,000 vulnerabilities affecting more than 30,000 technologies from more than 4,000 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. To provide enhanced insight into the evolving threat landscape, this volume of the report includes several new metrics, such as the window of exposure for Web browsers and the proportion of previously unseen malicious code. The full Internet Security Threat Report includes additional statistics and detail and is available for download at www.symantec.com/threatreport/. Broadcast media can download multimedia at www.thenewsmarket.com/symantec.

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 www.symantec.com.

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