Annual Symantec Internet Security Threat Report Reveals 81 Percent Increase in Malicious Attacks
Monday, April 30, 2012 04:01:00 AM (GMT)

http://media.marketwire.com/attachments/201010/647074_NI-SYM_Horiz_web300x79.jpg

Symantec Corp. (NASDAQ: SYMC) today announced the findings of its Internet Security Threat Report, Volume 17, which shows that while the number of vulnerabilities decreased by 20 percent, the number of malicious attacks continued to skyrocket by 81 percent. In addition, the report highlights that advanced targeted attacks are spreading to organizations of all sizes and variety of personnel, data breaches are increasing, and that attackers are focusing on mobile threats.

Read more detailed blog posts:

- The 2011 Internet Security Threat Report - There Is No Panacea to Protect Against All Attacks
- Keep Your SMB Safe from Internet-Based Threats

Malicious Attacks Continue to Grow Rapidly

Symantec blocked more than 5.5 billion malicious attacks in 2011, an increase of 81 percent over the previous year. In addition, the number of unique malware variants increased to 403 million and the number of Web attacks blocked per day increased by 36 percent.

At the same time, spam levels fell considerably and new vulnerabilities discovered decreased by 20 percent. These statistics, compared to the continued growth in malware, paint an interesting picture. Attackers have embraced easy to use attack toolkits to efficiently leverage existing vulnerabilities. Moving beyond spam, cyber criminals are then turning to social networks to launch their attacks. The very nature of these networks makes users incorrectly assume they are not at risk and attackers are using these sites to target new victims. Due to social engineering techniques and the viral nature of social networks, it's much easier for threats to spread from one person to the next.

Advanced Targeted Attacks Spread to Organizations of All Sizes

Targeted attacks are growing, with the number of daily targeted attacks increasing from 77 per day to 82 per day by the end of 2011. Targeted attacks use social engineering and customized malware to gain unauthorized access to sensitive information. These advanced attacks have traditionally focused on public sector and government; however, in 2011, targeted attacks diversified.

Targeted attacks are no longer limited to large organizations. More than 50 percent of such attacks target organizations with fewer than 2,500 employees, and almost 18 percent target companies with fewer than 250 employees. These organizations may be targeted because they are in the supply chain or partner ecosystem of a larger company and because they are less well-defended. Furthermore, 58 percent of attacks target non-execs, employees in roles such as human resources, public relations, and sales. Individuals in these jobs may not have direct access to information, but they can serve as a direct link into the company. They are also easy for attackers to identify online and are used to getting proactive inquiries and attachments from unknown sources.

Rise of Data Breaches, Lost Devices Concern for the Future

Approximately 1.1 million identities were stolen per data breach on average in 2011, a dramatic increase over the amount seen in any other year. Hacking incidents posed the greatest threat, exposing 187 million identities in 2011 -- the greatest number for any type of breach last year. However, the most frequent cause of data breaches that could facilitate identity theft was theft or loss of a computer or other medium on which data is stored or transmitted, such as a smartphone, USB key or a backup device. These theft-or loss-related breaches exposed 18.5 million identities.

As tablets and smartphones continue to outsell PCs, more sensitive information will be available on mobile devices. Workers are bringing their smartphones and tablets into the corporate environment faster than many organizations are able to secure and manage them. This may lead to an increase in data breaches as lost mobile devices present risks to information if not properly protected. Recent research by Symantec

shows that 50 percent of lost phones will not be returned and 96 percent (including those returned) will experience a data breach.

Mobile Threats Expose Businesses and Consumers

Mobile vulnerabilities increased by 93 percent in 2011. At the same time, there was a rise in threats targeting the Android operating system. With the number of vulnerabilities in the mobile space rising and malware authors not only reinventing existing malware for mobile devices, but creating mobile-specific malware geared to the unique mobile opportunities, 2011 was the first year that mobile malware presented a tangible threat to businesses and consumers. These threats are designed for activities including data collection, the sending of content, and user tracking.

Click to Tweet: Symantec blocked more than 5.5 billion attacks in 2011: http://bit.ly/K8NeJ8
Click to Tweet: #ISTR 1.1 million identities stolen per breach last year: http://bit.ly/K8NeJ8
Click to Tweet: Hackers exposed 187 million identities in 2011: http://bit.ly/K8NeJ8
Click to Tweet: Mobile vulnerabilities increased by 93% in 2011, #ISTR: http://bit.ly/K8NeJ8
Click to Tweet: Advanced targeted attacks spread to organizations of all sizes and information workers: http://bit.ly/K8NeJ8

Quote

"In 2011 cybercriminals greatly expanded their reach, with nearly 20% of targeted attacks now directed at companies with fewer than 250 employees," said Stephen Trilling, Chief Technology Officer, Symantec. "We've also seen a large increase in attacks on mobile devices, making these devices a viable platform for attackers to leverage in targeting sensitive data. Organizations of all sizes need to be vigilant about protecting their information."

Multimedia:

- Video: Did You Know: Internet Security Threat Report, Volume 17
- Podcast: Symantec Internet Security Threat Report Volume 17
- Webcast: Threat Update: Top Trends to Focus on for 2012
- SlideShare: Symantec Internet Security Threat Report 2011, Volume 17, April 2012
- Infographic: 2011 in Numbers
- Infographic: 2011 by Month

Resources:

- Full Report Home Page: Internet Security Threat Report, Volume 17
- Internet Security Threat Report Press Kit
- Build Your Own Customizable Version of the Internet Security Threat Report
- Blog Post: The 2011 Internet Security Threat Report - There Is No Panacea to Protect Against All Attacks
- Blog Post: Keep Your SMB Safe from Internet-Based Threats
- The Symantec Smartphone Honey Stick Project

Connect with Symantec

- Follow Symantec ThreatIntel on Twitter
- Follow Symantec on Twitter
- Join Symantec on Facebook
- Join Norton on Facebook
- View Symantec's SlideShare Channel
- Read Industry Trends on Delicious
- Subscribe to Symantec News RSS Feed
- Visit Symantec Connect Business Community

About the Symantec Internet Security Threat Report
The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in attacks, malicious code activity, phishing, and

spam.

About Security Technology and Response
The Security Technology and Response (STAR) organization, which includes Security Response, is a worldwide team of security engineers, threat analysts and researchers that provides the underlying functionality, content and support for all Symantec corporate and consumer security products. Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec Global Intelligence Network, which is made up of more than 64.6 million attack sensors and updates several thousand times every second. This network monitors attack activity in more than 200 countries and territories and tracks more than 47,000 vulnerabilities affecting more than 40,000 products from more than 15,000 vendors. Spam, phishing and malware data is captured through a variety of sources, including the Symantec Probe Network, Skeptic, Symantec.cloud and a number of other Symantec security technologies. The team uses this vast intelligence to develop and deliver the world's most comprehensive security protection.

About Symantec
Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.

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.

CONTACT: Ellen Hayes Symantec Corp (415) 407-5054 ellen_hayes@symantec.com Sherri Walkenhorst Connect Public Relations (801) 373-7888 sherriw@connectpr.com

Countries: US
Primary Identifiers: NLOK-US
Related Identifiers: NLOK-US