News Release

Yu Wui Wui
Symantec Corp.
+603 7623 2873
wuiwui_yu@symantec.com

Charmaine Goh/Zeck Pulle
ROOTS Asia Pacific
+603 7494 0272
charmaine.goh@rootsasia.com/
zeck@rootsasia.com

Symantec Internet Security Threat Report Reveals
Increase in Cyberespionage – Including Threefold Increase in Small Business Attacks

Malaysia Ranked 35th Among Countries Globally on Internet Threat Activities

KUALA LUMPUR, Malaysia – June 3, 2013 – Symantec Corp.'s (Nasdaq: SYMC) Internet Security Threat Report, Volume 18 (ISTR) today revealed a 42 percent surge during 2012 in targeted attacks globally compared to the prior year. Designed to steal intellectual property, these targeted cyberespionage attacks are increasingly hitting the manufacturing sector as well as small businesses, which are the target of 31 percent of these attacks. Small businesses are attractive targets themselves and a way in to ultimately reach larger companies via "watering hole" techniques. In addition, consumers remain vulnerable to ransomware and mobile threats, particularly on the Android platform.

"Cybercriminals aren't slowing down; they continue to devise new ways to steal information from organisations of all sizes. The sophistication of attacks coupled with today's IT complexities, such as virtualisation, mobility and cloud, require organisations in Malaysia and globally to remain proactive and use 'defense in depth' security measures to stay ahead of attacks," said Nigel Tan, director of Systems Engineering, Symantec Malaysia.

"While Malaysia is ranked 35th among countries globally on Internet threat activities, organisations should continue to take proactive initiatives to secure and manage critical information from a variety of security risks today. The top growing trends that organisations in Malaysia should watch out for in today's threat landscape includes targeted attacks in the manufacturing and small businesses sectors, mobile malware, and phishing threats," Tan added.

"Cybercriminals are targeting customer information, financial details and intellectual property. They have more ways than ever to spy on us, through computers, mobile devices and social networks. Any information they glean, from banking details to email addresses of associates, can be used in stealing identities and crafting further sophisticated attacks. One of the most significant innovations in targeted attacks is the emergence of

watering hole attacks. The attackers compromise the security of a website that an intended target is likely to visit and once the target visits the website, their computer becomes infected with malware," said David Rajoo, senior technical consultant, Symantec Malaysia.

Read more detailed blog posts:

- Information Unleashed: Internet Security Threat Report Volume 18
- Threat Intel: 2013 ISTR Shows Changing Cybercriminal Tactics
- The Confident SMB: SMBs – No Longer Invisible to the Bad Guys
- Ask Marian: Debunking Cyber Security Myths

Click to Tweet: #ISTR #SYMC 42 percent increase in targeted attacks in 2012: http://bit.ly/104R108
Click to Tweet: Small businesses are now the target of 31 percent of all attacks, a threefold increase from 2011: http://bit.ly/104R108
Click to Tweet: #ISTR #SYMC Mobile malware increased by 58% in 2012: http://bit.ly/14QWaO5

ISTR 18 Key Highlights Include:

Small Businesses Are the Path of Least Resistance

Targeted attacks are growing the most among businesses with fewer than 250 employees. Small businesses globally are now the target of 31 percent of all attacks, a threefold increase from 2011. While small businesses may feel they are immune to targeted attacks, cybercriminals are enticed by these organisations' bank account information, customer data and intellectual property. Attackers hone in on small businesses that may often lack adequate security practices and infrastructure. Web-based attacks globally increased by 30 percent in 2012, many of which originated from the compromised websites of small businesses. These websites were then used in massive cyber-attacks as well as "watering hole" attacks. In a watering hole attack, the attacker compromises a website, such as a blog or small business website, which is known to be frequently visited by the victim of interest. When the victim later visits the compromised website, a targeted attack payload is silently installed on their computer. The Elderwood Gang pioneered this class of attack; and, in 2012, successfully infected 500 organisations in a single day. In these scenarios, the attacker leverages the weak security of one business to circumvent the potentially stronger security of another business.

Manufacturing Sector and Knowledge Workers Become Primary Targets

Shifting from governments, manufacturing has moved to the top of the list of industries targeted for attacks in 2012. Symantec believes this is attributed to an increase in attacks targeting the supply chain – cybercriminals find these contractors and subcontractors susceptible to attacks and they are often in possession of valuable intellectual property. Often by going after manufacturing companies in the supply chain, attackers gain access to sensitive information of a larger company. In addition, executives are no longer the leading targets of choice. In 2012, the most commonly targeted victims of these types of attacks across all industries were knowledge

workers (27 percent) with access to intellectual property as well as those in sales (24 percent).

Mobile Malware and Malicious Websites Put Consumers and Businesses at Risk

Last year, mobile malware increased by 58 percent, and 32 percent of all mobile threats attempted to steal information, such as e-mail addresses and phone numbers. Surprisingly, these increases cannot necessarily be attributed to the 30 percent increase in mobile vulnerabilities. While Apple's iOS had the most documented vulnerabilities, it only had one threat discovered during the same period. Android, by contrast, had fewer vulnerabilities but more threats than any other mobile operating system. Android's market share, its open platform and the multiple distribution methods available to distribute malicious apps, make it the go-to platform for attackers.

In addition, 61 percent of malicious websites are actually legitimate websites that have been compromised and infected with malicious code. Business, technology and shopping websites were among the top five types of websites hosting infections. Symantec attributes this to unpatched vulnerabilities on legitimate websites. In years passed, these websites were often targeted to sell fake antivirus to unsuspecting consumers. However, ransomware, a particularly vicious attack method, is now emerging as the malware of choice because of its high profitability for attackers. In this scenario, attackers use poisoned websites to infect unsuspecting users and lock their machines, demanding a ransom in order to regain access. Another growing source of infections on websites is malvertisements—this is when criminals buy advertising space on legitimate websites and use it to hide their attack code.

Resources

- 2013 Internet Security Threat Report
- Press kit: 2013 Internet Security Threat Report
- Information Unleashed: Internet Security Threat Report Volume 18
- Threat Intel: 2013 ISTR Shows Changing Cybercriminal Tactics
- The Confident SMB: SMBs – No Longer Invisible to the Bad Guys
- Ask Marian: Debunking Cyber Security Myths

Connect with Symantec

- Follow Symantec on Twitter
- Join Symantec on Facebook
- Add Symantec on Google+
- Join Symantec Group on LinkedIn
- Read Symantec Corporate Blog Information Unleashed
- View Symantec's SlideShare Channel
- Subscribe to Symantec News RSS Feed
- Visit Symantec Connect Business Community

About the 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 Symantec's Global Intelligence Network, which Symantec analysts use to identify, analyse, and provide commentary on emerging trends in attacks, malicious code activity, phishing, and spam.

About Symantec

Symantec protects the world's information, and is a global leader in security, backup and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data centre, to cloud-based systems. Our world-renowned expertise in protecting data, identities and interactions gives our customers confidence in a connected world. 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.

FORWARD-LOOKING STATEMENTS: Any forward-looking indication of plans for products is preliminary and all future release dates are tentative and are subject to change. Any future release of the product or planned modifications to product capability, functionality, or feature are subject to ongoing evaluation by Symantec, and may or may not be implemented and should not be considered firm commitments by Symantec and should not be relied upon in making purchasing decisions.

Technorati Tags

Symantec, cybercrime, data breaches, malicious code, targeted attacks, hackers, Internet security, mobile threats, malware, watering hole attacks