Symantec Internet Security Threat Report Reveals Increase in Cyberespionage -- Including Threefold Increase in Small Business Attacks
Tuesday, April 16, 2013 04:01:00 AM (GMT)

LAS VEGAS, NV--(Marketwired - Apr 16, 2013) - **Symantec Vision 2013 --** Symantec Corp.'s (NASDAQ: SYMC) Internet Security Threat Report, Volume 18 (ISTR) today revealed a 42 percent surge during 2012 in targeted attacks 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.

"This year's ISTR shows that cybercriminals aren't slowing down, and they continue to devise new ways to steal information from organizations of all sizes," said Stephen Trilling, chief technology officer, Symantec. "The sophistication of attacks coupled with today's IT complexities, such as virtualization, mobility and cloud, require organizations to remain proactive and use 'defense in depth' security measures to stay ahead of attacks."

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: Ransomware is an emerging threat because of its high profitability for attackers: http://bit.ly/104R108
Click to Tweet: Web-based attacks increased 30 percent in 2012 #ISTR #SYMC: http://bit.ly/14QWaO5
Click to Tweet: One watering hole attack infected 500 organizations in a single day: http://bit.ly/14QWaO5
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 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 organizations' 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 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 organizations 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.

Multimedia:

- Video: ISTR Video
- Podcast: ISTR Podcast
- Webcast: ISTR Webcast
- SlideShare: ISTR 18
- Infographic: 2012 in Numbers
- Infographic: Attacks By Size of Targeted Organizations
- Infographic: Watering Hole Attacks
- Infographic: SMB
- Infographic: Fact or Fiction

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, analyze, 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 center, 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

CONTACT:
Ellen Hayes
Symantec Corp.
(415) 407-5054
Email Contact

Sherri Walkenhorst
Connect Public Relations
(801) 373-7888
Email Contact

Countries: US
Industries: Computers and Software, Computers and Software:Internet, Computers and Software:Software
Primary Identifiers: NLOK-US
Related Identifiers: NLOK-US
Subjects: Trade Shows/Seminars/Webinars