



MESSAGELABS INTELLIGENCE

THREAT PREDICTIONS FOR 2010

SECURITY TRENDS TO WATCH IN 2010

- **Antivirus is Not Enough** – With the rise of polymorphic threats and the explosion of unique malware variants in 2009, the industry is quickly realizing that traditional approaches to antivirus, both file signatures and heuristic/behavioral capabilities, are not enough to protect against today's threats. We have reached an inflection point where new malicious programs are actually being created at a higher rate than good programs. As such, we have also reached a point where it no longer makes sense to focus solely on analyzing malware. Instead, approaches to security that look to ways to include all software files, such as reputation-based security, will become key in 2010.
- **Social Engineering as the Primary Attack Vector** – More and more, attackers are going directly after the end user and attempting to trick them into downloading malware or divulging sensitive information under the auspice that they are doing something perfectly innocent. Social engineering's popularity is at least in part spurred by the fact that what operating system and Web browser rests on a user's computer is largely irrelevant, as it is the actual user being targeted, not necessarily vulnerabilities on the machine. Social engineering is already one of the primary attack vectors being used today, and Symantec estimates that the number of attempted attacks using social engineering techniques is sure to increase in 2010.
- **Rogue Security Software Vendors Escalate Their Efforts** – In 2010, expect to see the propagators of rogue security software scams take their efforts to the next level, even by hijacking users' computers, rendering them useless and holding them for ransom. A less drastic next step, however, would be software that is not explicitly malicious, but dubious at best. For example, Symantec has already observed some rogue antivirus vendors selling rebranded copies of free third-party antivirus software as their own offerings. In these cases, users are technically getting the antivirus software that they pay for, but the reality is that this same software can actually be downloaded for free elsewhere.
- **Social Networking Third-Party Applications Will be the Target of Fraud** – With the popularity of social networking sites poised for another year of unprecedented growth, expect to see fraud being leveraged against site users to grow. In the same vein, expect owners of these sites to create more proactive measures to address these threats. As this occurs, and as these sites more readily provide third-party developer access to their APIs, attackers will likely turn to vulnerabilities in third-party applications for users' social networking accounts, just as we have seen attackers leverage browser plug-ins more as Web browsers themselves become more secure.
- **Windows 7 Will Come into the Cross-Hairs of Attackers** – Microsoft has already released the first security patches for the new operating system. As long as humans are programming computer code, flaws will be introduced, no matter how thorough pre-release testing is, and the more complex the code, the more likely that undiscovered vulnerabilities exist. Microsoft's new operating system is no exception, and as Windows 7 hits the pavement and gains traction in 2010, attackers will undoubtedly find ways to exploit its users.
- **Fast Flux Botnets Increase** – Fast flux is a technique used by some botnets, such as the Storm botnet, to hide phishing and malicious Web sites behind an ever-changing network of compromised hosts acting as proxies. Using a combination of peer-to-peer networking, distributed command and control, web-based load balancing and proxy redirection, it makes it difficult to trace the botnets' original geo-location. As industry counter measures continue to reduce the effectiveness of traditional botnets, expect to see more using this technique being used to carry out attacks.
- **URL Shortening Services Become the Phisher's Best Friend** – Because users often have no idea where a shortened URL is actually sending them, phishers are able to disguise links that the average security conscious user might think twice about clicking on. Symantec is already seeing a trend toward using this tactic to distribute misleading applications and we expect much more to come. Also, in an attempt to evade antispam filters through obfuscation, expect spammers to leverage shortened URLs shorteners to carry out their own evil deeds.

- **Mac and Mobile Malware Will Increase** – The number of attacks designed to exploit a certain operating system or platform is directly related to that platform's market share, as malware authors are out to make money and always want the biggest bang for their buck. In 2009, we saw Macs and smartphones targeted more by malware authors, for example the Sexy Space botnet aimed at the Symbian mobile device operating system and the OSX.Iservice Trojan targeting Mac users. As Mac and smartphones continue to increase in popularity in 2010, more attackers will devote time to creating malware to exploit these devices.
- **Spammers Breaking the Rules** – As the economy continues to suffer and more people seek to take advantage of the loose restrictions of the CAN SPAM Act, we'll see more organizations selling unauthorized e-mail address lists and more less-than-legitimate marketers spamming those lists.
- **As Spammers Adapt, Spam Volumes Will Continue to Fluctuate** – Since 2007, spam has increased on average by 15 percent. While this significant growth in spam e-mail may not be sustainable in the long term, it is clear that spammers are not yet willing to give up as long an economic motive is present. Spam volumes will continue to fluctuate in 2010 as spammers continue to adapt to the sophistication of security software, the intervention of responsible ISPs and government agencies across the globe.
- **Specialized Malware** – Highly specialized malware was uncovered in 2009 that was aimed at exploiting certain ATMs, indicating a degree of insider knowledge about their operation and how they could be exploited. Expect this trend to continue in 2010, including the possibility of malware targeting electronic voting systems, both those used in political elections and public telephone voting, such as that connected with reality television shows and competitions.
- **CAPTCHA Technology Will Improve** – As this happens and spammers have a more difficult time breaking CAPTCHA codes through automated processes, spammers in emerging economies will devise a means to use real people to manually generate new accounts for spamming, thereby attempting to bypass the improved technology. Symantec estimates that the individuals employed to manually create these accounts will be paid less than 10 percent of the cost to the spammers, with the account-farmers charging \$30-40 per 1,000 accounts.
- **Instant Messaging Spam** – As cybercriminals exploit new ways to bypass CAPTCHA technologies, instant messenger (IM) attacks will grow in popularity. IM threats will largely be comprised of unsolicited spam messages containing malicious links, especially attacks aimed at compromising legitimate IM accounts. By the end of 2010, Symantec predicts that one in 300 IM messages will contain a URL. Also, in 2010, Symantec predicts that overall, one in 12 hyperlinks will be linked to a domain known to be used for hosting malware. Thus, one in 12 hyperlinks appearing in IM messages will contain a domain that has been considered suspicious or malicious. In mid 2009, that level was 1 in 78 hyperlinks.
- **Non-English Spam Will Increase** – As broadband connection penetration continues to grow across the globe, particularly in developing economies, spam in non-English speaking countries will increase. In some parts of Europe, Symantec estimates the levels of localized spam will exceed 50 percent of all spam.

ABOUT MESSAGELABS INTELLIGENCE

MessageLabs Intelligence is a respected source of data and analysis for messaging security issues, trends and statistics. MessageLabs Intelligence publishes a range of information on global security threats based on live data feeds from more than 14 data centers around the world scanning billions of messages and web pages each week. MessageLabs Team Skeptic™ comprises many world-renowned malware and spam experts, who have a global view of threats across multiple communication protocols drawn from the billions of web pages, email and IM messages they monitor each day on behalf of 21,000 clients in more than 99 countries. More information is available at www.messagelabs.com/intelligence.

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.

Copyright © 2009 Symantec Corporation. All Rights Reserved.

Symantec, the Symantec Logo and MessageLabs 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.

NO WARRANTY. The information contained in this report is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the information contained herein is at the risk of the user. This report may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice. No part of this publication may be copied without the express written permission of Symantec Corporation, 350 Ellis Street, Mountain View, CA 94043.

>EUROPE

>HEADQUARTERS

1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
Tel +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone 0800 917 7733
Support: +44 (0) 1452 627 766

>LONDON

3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Tel +44 (0) 20 7291 1960
Fax +44 (0) 20 7291 1937
Support +44 (0) 1452 627 766

>NETHERLANDS

WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801
Support +44 (0) 1452 627 766

>BELGIUM/LUXEMBOURG

Symantec Belgium
Astrid Business Center
Is. Meyskensstraat 224
1780 Wemmel,
Belgium
Tel: +32 2 531 11 40
Fax: +32 531 11 41

>DACH

Humboldtstrasse 6
Gewerbegebiet Dornach
Munich, Aschheim 85609
Germany
Tel +49 (0) 89 94320 120
Support :+44 (0)870 850 3014

>AMERICAS

>HEADQUARTERS

512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Tel +1 646 519 8100
Fax +1 646 452 6570
Toll-free +1 866 460 0000
Support +1 866 807 6047

>CENTRAL REGION

7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA
Tel +1 952 886 7541
Fax +1 952 886 7498
Toll-free +1 877 324 4913
Support +1 866 807 6047

>CANADA

170 University Avenue
Toronto, ON M5H 3B3
Canada
Tel :1 866 460 0000

>ASIA PACIFIC

>HONG KONG

Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: + 852 6902 1130

>AUSTRALIA

Level 13
207 Kent Street,
Sydney NSW 2000
Main: +61 2 8200 7100
Fax: +61 2 8220 7075
Support: 1 800 088 099

>SINGAPORE

6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: 800 120 4415

>JAPAN

Akasaka Intercity
1-11-44 Akasaka
Minato-ku, Tokyo 107-0052
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: + 852 6902 1130



Confidence in a connected world.

www.message-labs.com
info@message-labs.com