



MessageLabs Intelligence: 2009 Security Predictions

Security experts prepare for a year of morphing malware and phished social networks as scammers find new ways to exploit emerging environments

Having analyzed the global threat landscape for almost a decade, MessageLabs Team Skeptic™ is comprised of 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, emails and instant messages filtered by Skeptic™ each day.

Here are their security predictions for 2009:

Malware Makes Its “Mash-up”

The MessageLabs Intelligence team predicts that in 2009, Web 2.0 will provide an environment for contextual malware, which can consolidate multiple dynamic data streams to create a malicious environment from a number of diverse, unrelated sources.

Similarly, Malware-as-a-Service will emerge allowing the bad guys to request the type of malware they are seeking from an automated system and have it delivered instantaneously. Finally, malware will become more disposable as bad guys find newer and faster ways to change their malware so as to make it undetectable by newly adopted anti-virus systems.

Social Networking Gets Personal

Social networking sites will continue to be phished but in a much more professional way with a goal of collecting as much personal information and information surrounding a person's social network as possible to enable highly targeted and personalized spam. In 2009, spam will include proper names and will be segmented according to demographic or market. These same messages will be shorter with less content to filter and some will resemble legitimate newsletters and other special offers.

Reputation Hijacking Flourishes

Following on from the weakness in the fundamental design of the DNS (Domain Name Service) protocol that emerged in mid-2008 and afforded the opportunity to corrupt the cache of a DNS server, the MessageLabs Intelligence team predicts that phishing attacks will focus on exploiting vulnerable DNS domains and websites, and less on the traditional approach of hosting the easier-to-spot typo-like domains, where a cursory glance may not spot the fallible web address. Businesses will be expected to examine wider adoption of DNSSEC (DNS Security Extensions) as a means to mitigate potential DNS attacks.

CAPTCHA the Bad Guys

The bad guys accomplished the unthinkable in 2008 when broken CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) became the keys to the spamming kingdom. Spammers placed a premium on spamming with reputable online webmail as the messages are less likely to be blocked and allow spammers a world of possibility using an authentic email account. The MessageLabs Intelligence team predicts that while providers will respond to CAPTCHA breaking techniques in 2009 by enhancing the CAPTCHA process and deploying alternative CAPTCHA approaches, any web site that requires a personal account to be created online will continue to be targeted and the CAPTCHA failure rate will continue to increase accordingly.

419 Scams Lose Their Elaborate Prose

In 2009, Nigerian style 419, or advance fee fraud scams will become harder to recognize at first glance as the messages will contain only one or two sentences, rather than the rambling prose that has typically identified such scams. The true nature of the scam will be revealed slowly, as the target is invited to reply to find out more about the “business opportunity” offered. Additionally, scammers will also make greater use of email attachments to convey their messages with more detail, enabling the scam to bypass traditional anti-spam filters.

Globalization of Spam

Brazil, Russia, India and China are among the biggest emerging broadband markets worldwide and as such offer a tremendous opportunity for cybercrime. Through 2008, Internet use in China overtook that of the US. Based on this rapid growth and early spam samples, MessageLabs experts predict that in 2009 the emerging markets will be more heavily targeted with spam delivered in the local language. Growth in foreign language spam, especially Asian character spam, will increase by 100 percent from current levels at 5 percent to around 10 percent.

Mobile Mayhem

Attacks disguised as free application downloads and games have already targeted new smartphones in 2008. While these threats were more prank-like than truly malicious, 2009 will see mobile attacks become more malicious as criminals devise ways to make money by exploiting these devices further. Mobile attacks are far behind PC attacks with 300 mobile viruses in circulation compared with 400,000 for that of PCs but MessageLabs experts expect mobile attacks to parallel PC threats. For example, the “porndialers” of the last decade targeted PC users with modems, causing the infected PC to automatically dial premium-rate numbers established by the cybercriminals often replacing the owner’s ISP dial up number with an international number unbeknownst to the PC user until the phone bill arrived. Similarly, criminals will target mobile users in the same way, autodialing SMS texts to such numbers with the intent of bilking credit from the mobile user’s account.

Botnet Renaissance

In 2009, as the major botnets disrupted by the takedown of InterCage and McColo, at the end of 2008, seek to reassert themselves, it is expected that they will find replacement hosting services in a countries such as Russia, Brazil or China, and the botnets will be able to continue as before. The cyber-criminals will learn from this experience and this will precipitate an improvement in the technology behind many of these botnets, creating a new vanguard. The most sophisticated will take the form of hypervisor technology, where the malware will exist as a virtualization layer running directly on the hardware and intercepting some key operating system calls. This will mean that the “real” operating system, will be unaware of the existence of the underlying malware.

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 19,000 clients in more than 86 countries.

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.

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.

US: Marissa Vicario
Symantec Corp.
+1 646 519 8116
mvicario@messagelabs.com

EMEA: Paul Wood
Symantec
+44 (0) 1452 627705
pwood@messagelabs.com

APAC: Andrew Antal
Symantec
+61 2 8208 7171
aantal@messagelabs.com