



SECURITY FOCUS REPORT

---

# Spam in Today's Business World

## Introduction

Spam refers to unsolicited bulk email. These messages are used to advertise products and services for phishing purposes or to drive recipients to compromised or malicious sites with the intent of data or monetary theft. These have come a long way since their first incarnation as text strings. In the beginning, these were generally harmless to security-conscious recipients but now continue to pose threats, as these have become targeted and, therefore, more dangerous.

Web 2.0 platforms continue to pose endless possibilities for online communication, which unfortunately also translate to more avenues for cybercrime. Spam persists even in Web 2.0 platforms. In fact, these messages remain a great nuisance for Internet users. For most businesses, trying to mitigate this nuisance translates to profit loss. A recent study reported that these messages cost European companies an estimated US\$2.8 billion worth of productivity loss while U.S.-based companies reported a loss of US\$20 billion.

Over the years, spam has rapidly become a major security threat—a catalyst for potential financial drain or intellectual property theft—to organizations worldwide. This report will discuss current spam trends and related major incidents affecting the spam volume. It highlights how spammers have been leveraging social media as new means to scam users and to launch spear-phishing attacks. It also provides information on our next-generation security solutions to address the changing nature of spam, which goes beyond the scope of traditional email security.



## The State of the Current Spam Landscape

Almost 200 billion spam are sent every day, indicating an estimated hundredfold increase from 2.4 billion spam a day in 2002. Some 95 percent of these messages are sent by bots, the content of which is usually obfuscated and ambiguous.

### *THE SPAM VOLUME PLUMMETS*

The global spam volume in the first half of 2011 shows the varying number of spam intercepted on a weekly basis. Spam has proven costly in terms of resource such as bandwidth, server capacity, network infrastructure, and storage. These cost a company huge technological expenses due to items like the amount of email server processing power necessary to handle their deluge and the amount of time IT support staff need to spend to battle the problem.

Regardless of technique—botnet use or free email service abuse—the global spam volume presented below shows the varying states of malicious activity based on data our threat intelligence sensors gathered.

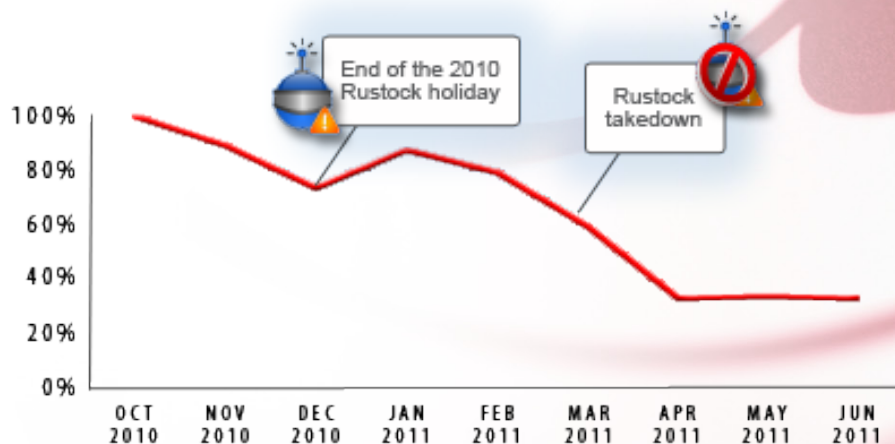


Figure 1. Global spam volume from October 2010 to June 2011

The 100 percent level represents the peak of the Rustock (i.e., one of the most notorious spambots) botnet's spamming activity seen during the second half of 2010. As shown, the number of spam constantly decreased in the middle of March 2011, following the decline during the 2010 holidays. Our researchers believe this could be attributed to the Rustock takedown. They developed a signature to identify spam originating from the botnet and found that in an hour after its takedown, the amount of traffic matching Rustock's signature dropped by 99.97 percent.

In the last 100 days of Rustock's operation, we saw more than 3 million distinct IP addresses sending out spam matching the botnet's signature. The number of infected systems was significantly smaller than this, as the majority of Rustock nodes were hosted on dynamic IP addresses. The botnet had approximately 1 million infected systems under its control, which were capable of sending out billions of spam every day. Since the spambot's discovery in 2006, Rustock was able to compromise thousands of systems and to send out billions of pharmaceutical spam.

The Rustock takedown severely reduced the spam volume close to the lowest number we previously recorded during the 2010 holidays. This shows that the overall spam volume on a monthly basis fell by about 40 percent compared with the highest number in October 2010. Before the plunge in December 2010, the spam volume remained relatively stable with little growth variations throughout the first half of 2010. Though the plunge appeared counterintuitive, considering the usual surge that takes advantage of the holiday online shopping spree, the low spam volume could be attributed to a decline in Rustock's activity. Because the spambot accounts for half of the overall spam volume, a decline in its activity automatically produced noticeable results.

The current state will eventually change, especially as spammers now focus on creating more targeted messages, aiming for "quality over quantity."

### *POSSIBLE RISE AFTER A BOTNET TAKEDOWN?*

It is encouraging to know that for several months after Rustock's takedown, the spam volume still has not risen, unlike after the 2008 McColo takedown. Before its takedown, McColo emerged as a major U.S. hosting service for international firms and syndicates involved in the remote management of millions of compromised systems for the sale of counterfeit pharmaceutical and designer goods as well as of fake security products via email. After the McColo takedown, the global spam volume continued to post small spikes, as spammers continued to use other botnets not hosted on the spambot.

TOP SPAM LANGUAGES

Trend Micro currently monitors 38 languages and dialects that are frequently used in spam. In the first half of 2010, we discovered that over 95 percent of the spam samples we collected were written in English. This trend continued in 2011, as English again topped the list of languages used with a 92 percent share.

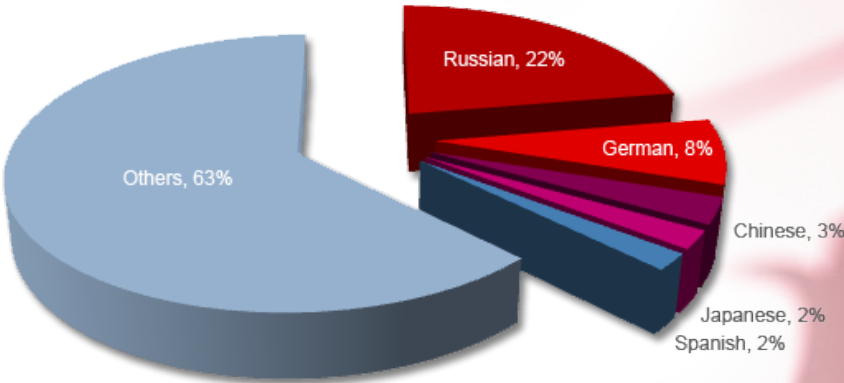


Figure 2. Top 5 non-English spam languages from January to June 2011

TOP SPAM-SENDING COUNTRIES

The top 5 spam-sending countries in the first half of 2011 accounted for one-third of the total spam volume. No single country, however, dominated the list.

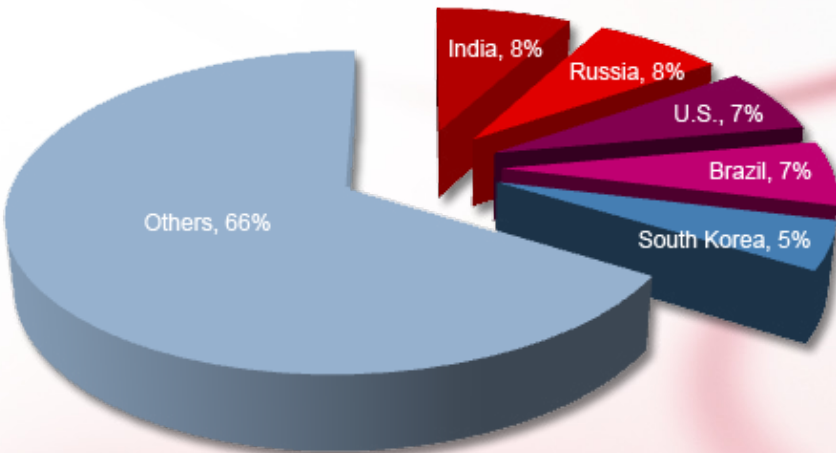


Figure 3. Top 5 spam-sending countries from January to June 2011

This year's numbers noticeably changed from last year. The United States topped the list of spam-sending countries in the first half of 2010 but slid down to third place in the first half of 2011. This decline coincided with the Rustock takedown last March, which implies that several of the spambots that have been taken down were based in the United States.

*SPAM ATTACHMENTS*

In July 2011, of the total volume, the average share of spam with malicious attachments per day was 2.14 percent. On August 13, 2011, data from our threat intelligence feed showed a huge spike, as 36.5 percent of the overall spam volume came with malicious attachments. Even though the majority of spam do not come with attachments, our researchers are currently seeing steady growth in the number of spam with malicious attachments, which started around the time this first exhibited a significant increase.



*Figure 4. Types of spam seen from January to June 2011*

Spam without attachments, including messages that have been embedded with malicious links, can be further classified into job, medical and commercial, and scam spam. Note that the Web reputation technology that comes with our messaging solutions protect Trend Micro product users from spam that come with malicious links.

Around 50 percent of the total number of spam come with attachments, notably using .ZIP as file extension name.

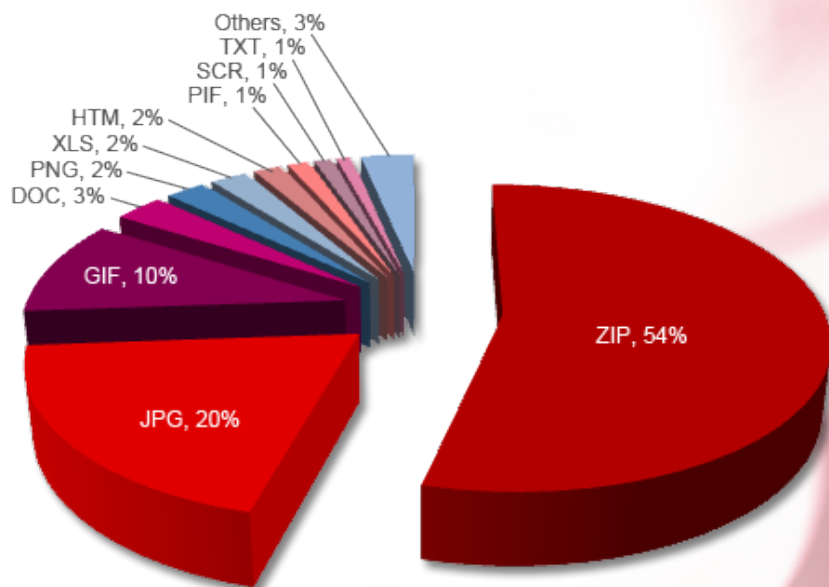


Figure 5. Top spam attachment types from January to June 2011

Apart from .JPG and .GIF image file attachments, spam can also carry *Microsoft Word* (.DOC) and *Excel* (.XLS) files as attachment. Sending .DOC and .XLS files as attachment gives spam, especially those supposedly from banks or legitimate service providers, greater credibility. Opening these attachments can lead to vulnerability exploitation in popular software like *Microsoft Word* or *Excel*, which exposes users to even more risks.

## Enterprise Spam Trends

Mass-mailed spam refers to messages that mostly promote fake pharmaceutical or fashion products or pornographic items intended for commercial gain. The way by which typical spam runs ensue has not changed for a long time but these still pose problems to enterprises in the form of increased bandwidth usage and mail server load.

Apart from serving various advertising purposes, spam runs also rely on social engineering techniques to carry out malicious intent. Social engineering, after all, is a simpler and more insidious way for cybercriminals to gain access to users' systems. Social engineering attacks are tailored to coincide with widely celebrated occasions, holidays, as well as trending news and other topics. Spammers typically use social engineering tactics for supposed ISP and Webmail service provider email notifications. These campaigns usually involve the secret installation of spyware or other malicious software or trick users into handing over their passwords and other sensitive financial or personal information.

## *DEALING WITH SPEAR PHISHING AND OTHER TARGETED ATTACKS*

From an enterprise point of view, new trends in the spam landscape go beyond the usual flooding of unsolicited bulk email. These trends include spear phishing, which is now being widely used by cybercriminals to obtain access to specific organizational targets.

Spear-phishing attacks target certain users, often the executives of huge corporations and high-ranking government officials who have access to confidential information such as proprietary company data and corporate banking credentials. A typical spear-phishing attack initially involves conducting research on who to specifically send a phishing email to in order to gain access to data that phishers normally steal. To do this, spear phishers spam several email accounts in a particular targeted company. They then identify which of the active accounts they will send phishing email to in order to get the information they need.

To a certain extent, behaviors such as conducting research on specific targets in order to infiltrate organizations, which are evident in spear phishing, are also common to most highly targeted attacks. In several instances, spear phishing can even be the first point of contact to launch a highly targeted attack wherein threat actors aggressively pursue specific targets, often through the use of social engineering, in order to maintain persistent control inside a network so as to extract sensitive information and to gain access to internal company networks.

Such was RSA's case in April 2011. RSA revealed details about an attack that used two different phishing email sent to its employees with the subject, "2011 Recruitment Plan." The attackers sent the said email to two small groups of RSA employees. These messages were crafted well enough to trick one of the employees into opening an attached *Excel* file that contained a zero-day exploit, which installed a backdoor program.

The data the cybercriminals obtained from RSA armed them with sufficient know-how to launch subsequent targeted attacks against the company's clients such as the International Monetary Fund (IMF).

A couple of weeks after the RSA breach, database marketing vendor, Epsilon, suffered the same fate, as the names and email addresses of its clients landed on cybercriminals' laps. This particular incident may have made it easier for attackers to design and consequently instigate spear-phishing attacks.

Organizations—regardless of industry—such as two departments of the Canadian government, the Oak Ridge National Laboratory, and the U.S. Department of Energy's Pacific Northwest National Laboratory (PNNL) followed RSA and Epsilon's footsteps, succumbing to near-crippling spear-phishing attacks.

Another risk that spear phishing brings is grave financial loss. Most of the targeted attacks that work are persistent and build upon the usual weak link—the social engineering ploy—wherein a human gets duped.

## THE RISE OF SPAM IN SOCIAL NETWORKING SITES

Spammers are moving into new fields by spreading other spam-like threats in social networking sites such as *Facebook* and *Twitter*. As in mass-mailing attacks, social media spam runs are triggered by the same motivation, albeit through a different platform.

Businesses that use social media platforms can come in contact with Web threats while using social networking sites for marketing and promotion. These may also cause system infections through employees who access sites such as *Facebook* and *Twitter* at work, presenting threats such as data loss or personal information theft. According to a [2010 global survey](#) that Trend Micro conducted, the number of social network users at work steadily rose from 19 percent in 2008 to 24 percent in 2010. As the number of employees who access social networks at work rises, the more viable social media spam attacks will become.



Figure 6. Page users see when they click links spammed in Facebook

A social media spam campaign we saw earlier this year made use of a script on *Facebook* to redirect users to a supposed new music player site feature. Clicking the link spammed in wall and chat messages redirected users to a site that tells them to follow several steps. Doing so eventually led to a scam site that informed users that they won a certain prize in exchange for giving out personal information.

Due to their wide popularity, social networking sites offer spammers a new venue to lure unwitting users into their traps. It is now easier and more effective to exploit human nature via social engineering than to exploit holes in software in order to gain access to personal information.

## The Battle Against Spam Continues

Traditional spam may be decreasing in volume but old techniques are still being used to instigate today's spam attacks so the battle continues. Attacks in social networking sites often utilize social engineering tactics, which cybercriminals have been leveraging since Webmail use became widespread. Users now receive more unsolicited messages via different channels while enterprises continue to repel multiple cyber attacks against their IT infrastructure.

### ANTICIPATING FUTURE CHALLENGES

At present, spamming methods have advanced to the point wherein IP blacklisting and content filtering on their own are no longer sufficient. Spammers are moving toward exploiting legitimate ISP mail servers for malicious purposes, which may require more comprehensive processes in terms of spam blocking.

Due to the exhaustion of existing IPv4 addresses, migration to its successor—IPv6—is inevitable. Mail service providers, however, warn that this migration will make it harder for them to filter spam from legitimate messages.

IPv4 was the foundation of most forms of Internet communication since 1981. IPv6 adoption may prove to be a hurdle to spam filtering, as tracking IP addresses back and blocking these will no longer be possible with the technology. The much larger address space of IPv6 will allow spammers to rapidly change addresses, something that was not possible with IPv4's more limited range. Spam filtering via IP blacklisting will thus be harder to do for IPv6 since spammers can easily change addresses without leaving a trace.

## How the Trend Micro Antispam Technology Works

The holistic, multilayered antispam solution of Trend Micro has a highly competitive spam detection capability powered by the Smart Protection Network™ technology. This technology continuously gathers global threat data from over 100 million nodes and correlates email, file, and Web threat information in the cloud to ensure automatic user protection wherever and however they connect.

The Smart Protection Network detects and prevents spam from even reaching organizations' networks via the email reputation technology. The Web reputation technology blocks user access to compromised or infected sites that may reach users via links in traditional or social media spam. Finally, the file reputation technology checks the reputation of each file against an extensive database before permitting user access. It also prevents the execution of malicious scripts and executable files that arrive as attachments to or via malicious links embedded in spam. These three reputation-based protection layers work together to prevent spam from even reaching users' inboxes.

IP reputation, a part of Trend Micro's email reputation technology, saves network bandwidth through IP filtering in that it searches for and blocks IP addresses that are known for sending spam even before these flood users' inboxes. The email reputation technology analyzes the history of an email server in order to give it a proper reputation rating. Email reputation technology is typically available as a centralized cloud service, queried on demand, allowing an email administrator to create policies to block or to delay the delivery of certain messages based on their senders' reputation rating. Using email reputation technology can save a company a considerable amount of resources, as this rejects up to 85 percent of all incoming email.

To minimize the occurrence of false positives, Trend Micro antispam solutions take proactive measures through high-performance heuristic content filtering, which involves manually scanning mail for various spam characteristics. Also part of the Smart Protection Network's proactive measures, machine learning automatically scans for indicators of good and bad messages, lessening false positives and catching more spam. This involves the use of a learning classifier technology based on complex mathematical algorithms, which aims to optimize "generalization" or the ability to correctly classify unseen data.

Trend Micro antispam learning systems are, therefore, capable of battling spam that show weak characteristics (i.e., spam that can easily pass off as legitimate messages). Its exceptional prediction power is also effective in that every spam it intercepts helps improve its system, resulting in better generalization performance; more robust behavior; and more effective and adaptive technology by automatically learning new tricks while adapting to changes.

Apart from proactive steps, our antispam solutions also use signature filters that combine a high-performance antispam engine and a wide spam signature database for more accurate detection. Signature-based scanning can be updated to block known spam sources while heuristic-based scanning can quickly adapt in order to detect entirely new spam categories or spamming methods. Fingerprinting or hashing also helps by blocking an incoming email if its fingerprint or hash key matches one on the database.

Enterprises should use a high-quality email reputation service as a first line of defense. This will reduce the number of email servers required to further process their remaining email traffic.

### *PROTECT YOUR SYSTEMS, PROTECT YOUR BUSINESS*

Enterprises will greatly benefit from investing in security solutions that are capable of securing systems and data alike. Based on our analysis, 3.5 new threats (i.e., malware, spam, and malicious URLs) are created every second. Given the speed at which threats are created combined with the malicious intent to defraud innocent users in order to steal data or money, a new set of technologies and methods need to be employed. It is crucial for employees to be educated about threats and threat mitigation as well as for organizations to focus not just on file-based threats like malware but also on incoming email threats, which are more likely to contain malicious URLs.

Over and above basic precautionary measures such as applying firewall settings and installing security solutions, enterprises need to roll out specific policies to ensure compliance throughout an organization. Enterprises should also use effective security solutions. Fortunately, several hardware, hosted software, and virtualized products that can be deployed to protect them from spam and the security threats these bring are readily available in today's market.

## References

- A.A. Zaidan, N. N. Ahmed, H. Abdul Karim, Gazi Mahabubul Alam, and B.B. Zaidan. (December 8, 2010). "Spam influence on business and economy: Theoretical and experimental studies for textual anti-spam filtering using mature document processing and naive Bayesian classifier." <http://www.academicjournals.org/ajbm/PDF/pdf2011/18Jan/Zaidan%20et%20al.pdf> (Retrieved August 2011).
- *Darknet.org.uk*. (June 13, 2011). "IMF (International Monetary Fund) Suffer Major Breach In Sophisticated Cyberattack." <http://www.darknet.org.uk/2011/06/imf-international-monetary-fund-suffer-major-breach-in-sophisticated-cyberattack/> (Retrieved September 2011).

- David Sancho. (April 11, 2011). *TrendLabs Malware Blog*. "Email Security After the Epsilon Incident." <http://blog.trendmicro.com/email-security-after-the-epsilon-incident/> (Retrieved September 2011).
- Gregg Keizer. (June 14, 2011). *Computerworld*. "Spear phishers sharpen skills, craft 'incredible' attacks, say experts." [http://www.computerworld.com/s/article/9217601/Spear\\_phishers\\_sharpen\\_skills\\_craft\\_incredible\\_attacks\\_say\\_experts/](http://www.computerworld.com/s/article/9217601/Spear_phishers_sharpen_skills_craft_incredible_attacks_say_experts/) (Retrieved September 2011).
- *IPv4 Countdown*. (2011). "Frequently Asked Questions about IPv4, IPv6 and the Internet." <http://www.ipv4countdown.net/frequently-asked-questions.php> (Retrieved August 2011).
- Jaikumar Vijayan. (July 6, 2011). *Computerworld*. "Second DOE lab is likely victim of spear-phishing attack." [http://www.computerworld.com/s/article/9218208/Second\\_DOE\\_lab\\_is\\_likely\\_victim\\_of\\_spear\\_phishing\\_attack](http://www.computerworld.com/s/article/9218208/Second_DOE_lab_is_likely_victim_of_spear_phishing_attack) (Retrieved September 2011).
- JM Hipolito. (November 15, 2008). *TrendLabs Malware Blog*. "Spam Volume Plummets as ISPs Pull the Plug on McColo." <http://blog.trendmicro.com/spam-volume-plummets-as-isps-pull-the-plug-on-mccolo/> (Retrieved August 2011).
- John Leyden. (March 8, 2011). *The Register*. "IPv6 intro creates spam-filtering nightmare: Blacklist extinction looms." [http://www.theregister.co.uk/2011/03/08/ipv6\\_spam\\_filtering\\_headache/](http://www.theregister.co.uk/2011/03/08/ipv6_spam_filtering_headache/) (Retrieved August 2011).
- Julie Ireton. (June 2, 2011). *CBC News*. "Hackers stole secret Canadian government data." <http://www.cbc.ca/news/technology/story/2011/06/02/pol-cyber-attacks.html> (Retrieved September 2011).
- Kim Zetter. (April 4, 2011). *Threat Level: Privacy, Crime and Security Online*. "Condé Nast Got Hooked in \$8 Million Spear-Phishing Scam." <http://www.wired.com/threatlevel/2011/04/condenast-hooked-by-spear-phisher/?asid=b1d80bb2> (Retrieved August 2011).
- Marco Dela Vega. (May 24, 2011). *TrendLabs Malware Blog*. "Facebook Spam Now Plays Your Favorite Music." <http://blog.trendmicro.com/facebook-spam-now-plays-your-favorite-music/> (Retrieved August 2011).
- Matt Yang. (January 11, 2011). *TrendLabs Malware Blog*. "Spam Levels Back to Preholiday Levels." <http://blog.trendmicro.com/spam-volume-back-to-preholiday-levels/> (Retrieved August 2011).
- Michael Horowitz. (April 7, 2011). *Computerworld*. "Spear Phishing: the real danger behind the Epsilon data breach." [http://blogs.computerworld.com/18093/spear\\_phishing\\_the\\_real\\_danger\\_behind\\_the\\_epsilon\\_data\\_breach](http://blogs.computerworld.com/18093/spear_phishing_the_real_danger_behind_the_epsilon_data_breach) (Retrieved September 2011).
- Raimund Genes. (June 27, 2011). *CTO Insights*. "The Human Factor of Targeted Attacks." <http://ctoinsights.trendmicro.com/2011/06/the-human-factor-of-targetted-attacks/> (Retrieved August 2011).

- Richard Boscovich. (March 17, 2011). *The Official Microsoft® Blog*. "Taking Down Botnets: Microsoft and the Rustock Botnet." [http://blogs.technet.com/b/microsoft\\_blog/archive/2011/03/17/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx](http://blogs.technet.com/b/microsoft_blog/archive/2011/03/17/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx) (Retrieved August 2011).
- Trend Micro, Incorporated. (July 2010). *TrendWatch*. "TrendLabs Global Threat Trends 1H 2010." [http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/tm101hthreat\\_report.pdf](http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/tm101hthreat_report.pdf) (Retrieved August 2011).
- Trend Micro, Incorporated. (July 12, 2010). *Trend Micro Newsroom*. "Trend Micro Teams with VMware to Offer VMware vShield™ Endpoint Solution for Agentless Security in Virtualized and Cloud Environments." [http://trendmicro.mediaroom.com/index.php?s=43&news\\_item=822&type=archived&year=2010](http://trendmicro.mediaroom.com/index.php?s=43&news_item=822&type=archived&year=2010) (Retrieved August 2011).
- Uri Rivner. (April 1, 2011). *Speaking of Security: The Official RSA Blog and Podcast*. "Anatomy of an Attack." <http://blogs.rsa.com/rivner/anatomy-of-an-attack/> (Retrieved August 2011).



#### ABOUT TRENDLABS<sup>SM</sup>

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to:

- Continuously monitor the threat landscape across the globe
- Deliver real-time data to detect, to preempt, and to eliminate threats
- Research and analyze technologies to combat new threats
- Respond in real time to targeted threats
- Help customers worldwide minimize damage, reduce costs, and ensure business continuity



Securing Your Journey  
to the Cloud

#### ABOUT TREND MICRO<sup>SM</sup>

Trend Micro, Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our website at [www.trendmicro.com](http://www.trendmicro.com).

#### TREND MICRO

10101 N. De Anza Blvd.  
Cupertino, CA 95014

US toll free: 1 +800.228.5651  
Phone: 1 +408.257.1500

Fax: 1 +408.257.2003  
[www.trendmicro.com](http://www.trendmicro.com)