



Table of Contents

January 2008

Secure Computing® brings you the latest SecureNews.

In this SecureNews:

Breaking news

- [Secure Computing Named Worldwide Leader in the Web Security Appliance Market](#)
- ~ [Analyst Webcast: Stay Out of the Headlines with PCI Compliance](#)
- ~ [Coming to a city near you...Secure Computing's complimentary Lunch & Learn series](#)

SecureAlerts

- ~ [Secure Computing Research Announces New Enhancements to TrustedSource.org](#)
- ~ [FTC Report Says Spam Is Significant Factor in Malware and Financial Crime](#)
- ~ [Storm Worm Continues to Morph](#)


Product corner

- ~ [Secure Computing Unveils SafeWord 2008](#)
- ~ [Secure Computing's Webwasher Anti-Malware Engine Beats Leading Vendors to Win Top Honors in Comparative Review](#)
- ~ [SC Magazine Names Sidewinder 7.0 and IronMail "Best Buys" for 2007](#)

Breaking news

Secure Computing Named Worldwide Leader in the Web Security Appliance Market

According to leading market research firm IDC, **Secure Computing is the worldwide revenue leader for Web security appliances.** New data in the December 2007 IDC report, "Worldwide Web Security 2007-2011, and 2006 Vendor Shares" shows that Secure owns a larger share of the Web security appliance market **than all other vendors, including Websense, Trend Micro and Symantec.**




IDC's definition of Web security includes Web filtering, Web anti-malware, Web application firewall, and Web content filtering products. Web security products are deployed on software, appliance and hosted service platforms. Web security products protect against both inbound (malware) and outbound (data leakage) threats.

[Read the full announcement](#)

Breaking news


Analyst Webcast: Straight Talk on PCI Compliance



WEBCAST: Straight Talk with IDC:

How to Stay Out of the Headlines with PCI Compliance

Date: January 31, 2008
Time: 1:00pm - 2:15pm EST



With the recent rise in data breaches of credit card information and rising identity thefts, implementing a sound information security program is no longer optional. **Companies processing credit card information must embrace and implement sound data protection strategies to ensure the confidentiality and integrity of customers' payment information.** The cost of compliance, while significant, is far less

expensive than the cost of remediation, where public outcry and media coverage of a breach could damage a company's brand irreparably.

Worldwide news

- [SecureNews / Monthly News Highlights](#)

Join IDC and Secure Computing for this webinar and discover:

- What are the benefits of PCI compliance to your organization
- What are the costs of PCI compliance (implementation vs. remediation)
- What implementation challenges do companies face and how to overcome them
- Which technology solutions map to the various PCI requirements
- What are the best practices for organizations to achieve PCI compliance
- Actual case studies and examples of companies who are already PCI compliant

Featured Speaker: Chris Christiansen, IDC Program Vice President, Security Products and Services

Date: Thursday, January 31, 2008

Time: 1 pm ET

Length: 75 minutes

[Register now](#) to reserve your spot!

Learn more about PCI Compliance at [Secure Computing's PCI site](#).

Breaking news

Coming to a city near you...Secure Computing's complimentary Lunch & Learn series

Lunch & Learn with Secure Computing



Topic: Web 2.0 Security Threats

You're invited to join Secure Computing® for lunch while we share with you cutting-edge information about the latest Web 2.0 security threats. Discover how companies are successfully addressing these threats through the Secure Web 2.0 Anti-Threat Initiative - SWAT.

Cities we're hosting Lunch & Learns in from January 23rd to February 21st: Bellevue, Charlotte, Denver, Hartford, Houston, Los Angeles, Louisville, Melville, Rochester, Salt Lake City, Scottsdale, St. Louis, and Tampa.

[Please visit our Lunch and Learn Web page on our SWAT site for dates, locations, and to register!](#)

Looking for more information about Web 2.0 threats and protection strategies? Check out our [Secure Web 2.0 Anti-Threat site](#).

The TrustedSource.org site features several improvements to provide our customers and the general public with the most current intelligence on global security threats and trends.



- **Global Intelligence for Mail Volume and Spam:** The TrustedSource™ homepage includes a new interactive global mail volume/spam tracking graph that shows the total global message volume and its relationship to the total amount of spam. An interactive timescale slider allows the user to view the data by different time intervals.
- **Storm Tracker:** The Storm Worm has been the major threat in 2007. The Secure Computing® Research team tracks the latest activities of this threat daily and provides a comprehensive view of it. Users can get daily stats-at-a-glance on the number of new Web proxy IPs that Storm is using, the most active Storm Web proxy IPs, newly active Storm Web proxy IPs, the geo-location of Storm Web Proxy IPs, and the top domains sending Storm threats. For more information, please visit our [Storm Tracker](#) Web page on TrustedSource.org.
- **Research Blog:** Secure Computing Research continues to offer insights on the latest threats through a variety of means including blogs. The most recent entries from the informative [TrustedSource Research Blog](#) can now be viewed by scrolling down the TrustedSource homepage.
- There are several new features for users that [sign up for a free login](#) to TrustedSource.org.
 - **Malware Alert Service:** TrustedSource.org tracks the latest malware threats. Users can now subscribe to an email alert that will be sent to them any time TrustedSource has information on a new malware outbreak. Users can also request the information in a digest form sent daily, weekly, or monthly.
 - **Ask the Expert:** Users can now get questions answered concerning the latest security threats directly from the Secure Computing Research team. The service is called 'Ask the Expert.' The most interesting questions will be posted to the Web site for the benefit of all.
 - **Give Us Your Feedback:** In an effort to continue to offer the features our users want, TrustedSource.org now has a section for subscribers to submit ideas on how to improve the Web site. These ideas will be considered by the Research team for future enhancements to the site.

We invite you to check out these enhancements at TrustedSource.org today!

The Federal Trade Commission released its report this month on the state of spam and phishing. The report described the findings of a **July 2007 panel workshop, “Spam Summit: The Next Generation of Threats and Solutions.”** According to the report, the nature of spam has shifted, and the newest generation of spam is perpetrated as a criminal enterprise. The report also notes that spammers have not only changed their motives, they have also changed their methods.

SECUREALERTS

Motivation, according to the FTC, has changed **the nature of spam from merely being annoying, to being a “vector for criminal activity.”** Several scenarios are highlighted, including spam that directs victims to Web sites that trick them into revealing passwords or financial data, install keylogger software, or hijack computers for use in the botnet. In recognition of this criminal factor, the FTC has brought **over 90 law enforcement actions** as of November 2007 relating to spam.

The report says that the **greatest methodological shift has been the use of malicious bots, which take control of thousands of computers and use them to send out huge volumes of spam.** Most of the time, **owners of the zombie computers are completely unaware** that their PCs are being used in such a way. The Panel also reported that **bots are responsible for 95 percent of all spam.**

In addition to the use of botnets, the report noted the **growing phenomenon of “fast flux,” a technique where infected bot computers are used as proxies or hosts for malicious Web sites** for the purpose of disguising the true origin. Using this technique, IP addresses can be rotated regularly.

The panel also made note of the fact that criminal spam enterprises are growing because of the simplicity of doing business. Modern phishing software and crimeware is widely available and cheap, allowing even unsophisticated criminals to create and launch a malicious spam campaign. In addition to cheap tools, botnets are also widely available for rent by the hour.


Going beyond analyzing the methods and motives, **the Commission also took note of techniques that have proven effective in combating spam. These techniques include spam filtering technologies, email authentication techniques, and reputation-based technology.**

The creation of domain-level email authentication systems would thwart the ability of spammers to send email anonymously. In addition to domain-level email authentication schemes, the report specifically discusses the promise of accreditation and reputation services. An accreditation service certifies that a sender uses a given set of best practices, while a reputation service, such as TrustedSource™ from Secure Computing®, examines the practices of all email senders, and assigns a reputation score to each one. The report states that “Panelists agreed that reputation services are critical building blocks, and that reputation is an important component in minimizing the impact of spam in the inbox.”

To learn more, please refer to the following papers from Secure Computing:

1. [Internet Risk Management in a Web 2.0 World](#), our commissioned study by Forrester Consulting
2. [TrustedSource: The Next-Generation Reputation System for Enterprise Gateway Security](#)
3. [Preventing New Spam Technologies from Infiltrating Your Network](#) paper

Additional Secure Computing papers can be found [here](#).



Storm Tracker

The infamous Storm worm is showing no signs of slowing down, and continues to wreak havoc on the Internet. Demonstrating precisely what Grinches the perpetrators are, on Christmas Eve, the SANS Internet Storm Center issued a warning about an anticipated Storm-bot attack, warning readers that a new wave of emails was being sent out to expand their rapidly-growing botnet. Through the guise of a Christmas theme, the email extended an X-rated offer, and victims were directed to an infected Web site called merrychristmasdude.com. Emails featured subject lines including "Merry Christmas to All", "Warm up this Christmas", "Mrs. Clause Is out Tonight!", "The Twelve Girls of Christmas", "Jingle Bells, Jingle bells", and "Cold Winter Nights." Once a victim visits the site, their PC is infected with the latest version of the Storm worm.

According to SANS, the domain was based in Russia, and hosted on a "fast-flux" network of over 1,000 nodes. This technique attempts to thwart anti-security measures by registering and subsequently de-registering addresses. The strategy hides the IP address of the rogue site by constantly switching between infected slave machines that are used as proxies. The binary changed every 15 minutes to update the peer list used by the botnet. The Storm worm is alternately referred to as either Nuwar or Peacomm.

After releasing the Christmas spam barrage, the perpetrators moved on to New Years wishes, with subject heading that included "Happy 2008!" AND "Happy New Year!". This time, the messages attempted to trick users into clicking on a URL by making them believe they had received an electronic greeting card. The rogue Web site, uhavepostcard.com, featured a file called happy2008.exe, which instead of a greeting card, released yet another variant of the Storm worm. The New Year version also added a rootkit, which makes the worm easier to hide itself from anti-virus software.

The trickiness factor of the perpetrators of Storm underscores the necessity of rolling out a multi-factor strategy to combat viruses and other malware, which include anti-virus software, URL filtering, reputation-based protection, and educating users to never click on URLs from within the body of an email.

Check out Secure Computing Research's **Storm Tracker** Web page on www.trustedsource.org to learn the latest information and statistics about the Storm worm and the threat it poses to individuals and organizations.

To learn more, please read our *Spam Threat Alert* paper or Did You Get the Memo? **Getting You from Web 1.0 to Web 2.0 Security**

Additional Secure Computing papers can be found [here](#).



The Best Two-Factor Authentication Solution for Microsoft Windows Environments



Secure Computing is pleased to announce the release of **SafeWord 2008**, a new version of the company's **SafeWord two-factor authentication solution**. Designed for 64- and 32-bit Windows platforms, SafeWord 2008 two-factor authentication protects an organization's most important assets and applications. SafeWord's easy-to-use tokens and seamless integration with your existing Microsoft infrastructure make it simple-to-deploy two-factor authentication for VPNs, Citrix applications, Web applications, Webmail, and Outlook Web Access. SafeWord tokens never expire and come with a lifetime warranty.

SafeWord 2008's **Enterprise Solution Pack** add-on allows you to deploy and protect more applications, enables the use of your phone as a two-factor authenticator, and lowers TCO through tools that make deployment simple for your administrators and users. **SecureWire Access Gateway, included with Enterprise Solutions Pack, provides a fully featured SSL VPN and Web access gateway for unlimited users.**

See the [SafeWord 2008 Product Overview](#) for more information.



Secure Computing's Webwasher Anti-Malware Engine Beats Leading Vendors to Win Top Honors in Comparative Review

In an independent test, Secure Computing's Webwasher Anti-Malware engine ranked first place, surpassing all of the leading vendors and scoring higher than 26 other companies as the top



product for detecting malware. The research, conducted by independent AV Test Labs (www.av-test.org) and published in November, mirrored the true magnitude of malware threats and illustrated the varying degrees of effectiveness of anti-malware products in detecting these threats. The test bombarded each solution with over one million different malicious files from the past 6 months and evaluated malware detection capabilities performed on Windows XP. With a combination of Trojans, backdoors, and bots (zombies) to detect, **Secure Computing's Webwasher technology emerged as the clear winner, detecting 99.45 percent of the malicious files.** These lab results demonstrate the superior ability of Webwasher to effectively secure users in a hazardous threat landscape.

[Read the press release.](#)

Product corner

SC Magazine Names Sidewinder 7.0 and IronMail
"Best Buys" for 2007



SECURE COMPUTING®
IronMail®
Messaging Gateway Security

SECURE COMPUTING®
Sidewinder®
Network Gateway Security

SC Magazine's technology experts have made their choices for the **best products of 2007** from among the dozens of entries that were subjected to thorough group tests and reviews during the year, and have singled out two Secure Computing products for distinction. **Sidewinder 7.0 and IronMail were each named a "Best Buy" in their respective categories of Firewall and the Email Content Filtering.** SC Magazine awards the Best Buy designation to products that SC Lab rates as outstanding.

[View SC Magazine's "Best of 2007"](#)

Worldwide news

SecureNews Monthly Press Highlights

Although the infamous Storm worm enters 2008 with a reputation as the world's most dangerous botnet, security experts say there's an up-and-comer called Nugache that could give it a run for its money, according to this [Network World article](#). [TechNews World](#) reports that end users who click on seemingly legitimate Google ads may be at risk of infection by a Trojan that substitutes rogue ads for the real thing. Google and the companies that pay for genuine ads are also victimized, because the pretenders usurp traffic and potential revenue.

