Anti-Spam Experts Identify Top Five Ways Proven to Classify and Stop Spam

Submitted by: eclat Marketing

Friday, 9 May 2003

SurfControl's Anti-Spam Team Releases Expert White Paper Providing Today's Enterprises with New Information and Techniques to Battle and Win the War Against Spam.

Congleton, UK , (May 8, 2003) - Anti-spam experts at the world's number one Web and e-mail filtering company, SurfControl (London:SRF, Nasdaq Europe: SRFC), released today the top five ways proven to identify and stop spam in the enterprise. The methods, state-of-the-art technologies available to today's IT executives, are identified in a new white paper, "Major Techniques for Classifying Spam."

Written by a team of e-mail filtering experts at SurfControl, the white paper comes as more and more people agree that it will take a combination of advanced technology and a new legal infrastructure to effectively fight spam. Paris Trudeau, a White Paper author and SurfControl E-mail Filter Product Marketing Manager who regularly advises enterprises on ways to combat spam, says that increasingly effective software tools are capable of correctly identifying and filtering a large percentage of spam e-mails.

"The key," Trudeau says, "is to find ways to maximise the accuracy of identifying spam with the least amount of human intervention, which can be enormously costly. To do this, organisations need to use multiple spam detection and classification technologies that analyse and filter actual e-mail content automatically and in real time to stop spam at the network edge." Customisation is also important, she added. "One company's spam is another's legitimate business e-mail."

Top Five Ways Proven to Classify and Stop Spam:

1. Fingerprint Database Analysis
2. Lexical Analysis
3. Artificial Intelligence
4. Statistical Analysis
5. Heuristics

Fingerprint Database Analysis for spam is similar to fingerprint-based identification common in anti-virus software, and is very effective in identifying known spam strains and is unlikely to identify an innocuous message as spam. Lexical Analysis examines words and phrases within message content in the context of the whole e-mail, which is necessary, the authors note, "because spam messages are constantly mutating to avoid detection." Artificial Intelligence using neural networks that can be trained to learn what an organisation defines as spam. Statistical Analysis, a method similar to AI, can be trained to weight the overall probability that a message is spam. Heuristics, a term with Greek origins that means "to find," is a framework that combines the results of spam identification tests, determines an overall score of a message's content and ultimately identifies a message as spam or not.

In addition to these content technologies, Dr. Richard Cullen, a second paper author who is a senior developer on SurfControl's e-mail filtering development team, says it is important to focus on the actual transport of the spam as well. "It is important to completely disable the open relay functionality of any Internet mail server," Cullen said. "External users - including spammers - must never be allowed to send messages through the mail server without verifying user authentication to that server's users."

"SurfControl is the only company offering the unique combination of the top five technologies which produce the best and most accurate e-mail filtering results for the enterprise," Cullen said.

SurfControl E-mail Filter technology combines multiple layers of spam detection and content filtering, including a vast spam signature database to identify and classify spam in real time, artificial intelligence and Boolean logic. It also includes some of the industry's strongest anti-virus protection, to scan, cleanse and block e-mail borne viruses, by file type and in attachments. It also gives companies the ability to assess e-mail content risk in an offline production environment with E-mail Audit to review historical e-mail communication without having to reconfigure their current network settings. E-mail Audit provides organisations with insight into exposure to potential risks and can help them develop effective acceptable use policies.

To obtain a copy of SurfControl's White Paper, go to:

  <http://www.surfcontrol.com/general/assets/whitepapers/4ClssfySpm_Apr03.pdf>

Press contacts:

Natasha Staley
Eclat Marketing
0118 989 5601
natasha@eclat.co.uk

Gemma Lewis
Eclat Marketing
0118 989 5604
gemma@eclat.co.uk

About SurfControl

SurfControl plc, the world's number one Web and e-mail filtering company, is the only company in the security market offering a total content security solution that combines Web and e-mail filtering technology with the industry's largest, most accurate and relevant content database and adaptive reasoning tools to automate content recognition. SurfControl is the leading content security company in the secure content management market, a market analysts expect to reach nearly $5 billion by 2006.

SurfControl's Internet monitoring and policy management solutions are flexible, scaleable and interoperable to meet the diverse needs of all its markets -- corporate, education, home and OEM. SurfControl, which can be installed in any network environment, offers a choice of platform independent or integrated solutions. SurfControl has world-class partners, including Microsoft, Check Point, Cisco, IBM and Nokia, as well as a customer base that includes many of the world's largest corporations.

The company offers the most sophisticated yet easy to use technology, the best understanding of market needs and a global reach unmatched in the industry. SurfControl has been recognized as the fastest growing company in the North of England at the U.K. Deloitte & Touche 2002 Technology Fast 50, and was honored as Company of the Year at the 2002 techMARK Awards.

For further information and news on SurfControl, please visit

http://www.surfcontrol.com/

Natasha Staley
Senior Account Executive
éclat Marketing
natasha@eclat.co.uk

Tel: 0118 989 5600
Mob: 07899 957022
Fax: 0118 989 5656
Web: http://www.eclat.co.uk

response**source**