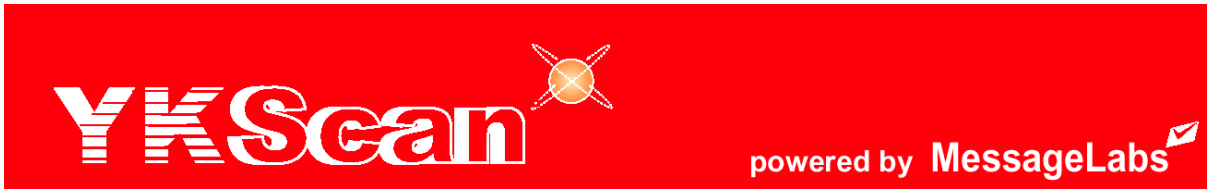
Yui Kee Computing Ltd.

Newsletter

August 2002

Contents



MessageLabs Protects Cathay Pacific Holidays

Cathay Pacific Holidays' Lotus Notes email system connects the company to 5000 members, 600 hotels and over 40 Cathay Pacific offices. Previously, the system suffered from virus outbreaks almost four times a year, and daily operations had been badly affected.

Unsatisfied with the disruptions, Cathay Pacific Holidays' General Manager Patrick Yeung and IT Manager Gemini Wong set out four improvement objectives – anti-virus, anti-spam, email backup and content filtering. Mr. Yeung's main concern was not cost, but ease-of-use. They chose MessageLabs, which scans all incoming emails through its 22 control towers throughout the world, before they reach the company's server. MessageLabs' proprietary Skeptic technology will detect the latest virus before any anti-virus companies learn of it.

Mr Wong said it only took them 50 minutes to get MessageLabs' service up and running. It was only necessary to ask their ISP to change the DNS MX record to route all email through MessageLabs' control towers. There was no need to install any software or hardware. There is no initial investment, just a monthly subscription fee. Since implementing MessageLabs' service over 5 months ago, Cathay Pacific Holidays has not been affected by a virus attack.

Yui Kee provides MessageLabs anti-virus, anti-spam and anti-porn service to its customers as YKScan.

Bug in e-Cert User Software

Current users of Hongkong Post e-Certs will find it useful to know that the latest version of the user software, 2.0, which is sent to renewal applicants is incapable of being used for

downloading a renewal certificate. The software is sent on a CD marked HK Post e-Cert User Software 02/02 M020113. Affected users should contact Hongkong Post technical support before downloading their renewed certificate.

Hongkong Post reports that it is working on a fixed version.

BBC Warns about Microsoft Bugs

Graham Cluley urged users to download the latest updates from Microsoft's Windows Update site. See http://news.bbc.co.uk/2/hi/technology/2211571.stm for the full story.

2002 - Viruses on the Decline

Reprinted under permission from the Aladdin Knowledge Systems CSRT (Content Security Research Team).
http://www.esafe.com/home/CSRT

While this year was marked by the most destructive and clever Klez virus, if we look back we can clearly see there have been no other major outbreaks and the entire virus-making "industry" is on the decline. Klez ruled the top ten viruses this year and very far behind it were threats such as Lentin and the Frethem family. This list is dwarfed when compared to last year's most notorious threats: Badtrans, Code Red, Hybris, Nimda and last year's "champion" - SirCam.

The reasons for this decline are speculated to be the result of increased awareness of the subject. On one hand, Internet users tend to be more cautious, many of them recognizing potential virus infections by sight alone. On the other hand, the anti-virus industry has learned a great deal from last year's experience and nowadays the protection offered by anti-virus software became much more effective. As a result, virus makers have to work harder in order to create actual threats - ones that can fool both users and software.

One must always keep in mind, however, that better security means less criminals - but the ones left only try harder.

… Or Still Growing?

Comment by Allan Dyer

It is not difficult to find reports that contradict Aladdin's conclusions, in May Messagelabs reported that Klez had become the biggest computer virus ever, Symantec report on a group of new Peer-to-Peer worms in their August newsletter, and Sophos detected and protected against 3,279 new viruses in the first six months of 2002. Messagelabs also said it intercepted more than 2 million infected messages in the first six months of 2002, double what it encountered in the same period last year.

Where is the truth? Reality is never as simple as nice, clean statistics. Messagelabs customer base has been steadily growing as more people realise the benefits of their service - they recently announced their one millionth user, so the important figure to look at in their statistics is not the total number caught, but the ratio of viruses to total emails. That has also grown, but not as fast. Sophos also said that it detected and protected against 6,127 new viruses in the first half of 2001, almost twice as many as this year. However, the number of new viruses is largely irrelevant to the threat level - most of the incidents last year were caused by a handful (Badtrans, Hybris, CodeRed, Sircam and Nimda) of viruses - less that 0.1% of the total number of new viruses. Today, the discrepancy is even more pronounced: Sophos's figures show that just one virus, Klez, accounts for 29.4% of incidents, and Messagelabs' catch for the last 24 hours show 19538 out of the 31964 viruses they stopped were Klez - that is 61%.

But this is not the whole picture either: Messagelabs' figures, because they are specialised in email services, only counts the viruses in email - there could be a massive outbreak of the Peer-to-Peer worms mentioned by Symantec, and, as long as they did not also target email, Messagelabs' statistics would show nothing. Sophos' figures only show incidents reported to them. There are no really reliable, global statistics for computer viruses and worms.

What is my view? Things are getting worse: CodeRed and Nimda showed the potential of worms, Sircam and Klez showed how bad many users are at following guidelines. The drop in the number of new viruses is unimportant, and could rapidly change (we once saw the virus total jump by 17,000+ overnight, because some idiot ran a virus generation toolkit for a very long time, and dumped the results on the anti-virus developers). However, protecting yourself and your organisation is still the same: follow sound security practices.

Free HACK Expo starts next Wednesday

Don't forget to come and visit us on stand number 16 at the HK Convention and Exhibition Centre next Wednesday, when the HACK expo will be held. You'll have the chance to take part in a lucky draw, meet leading white-hat hacker Rain Forest Puppy, and attend free seminars and product demonstrations. Allan Dyer will be speaking at a free seminar - check the details at the Expo.

If you don't want to queue on the day, just visit http://www.hackexpo.com/ and fill in the online expo registration form there.

MessageLabs launches next generation anti-spam service

MessageLabs applies revolutionary anti-virus technology to let firms control what gets through.

- Inability to define what constitutes spam seen as root of problem
- 10% of every working day in UK spent dealing with spam
- Survey shows 58% of US Business Managers unable to manage spam

Yui Kee is now supplying MessageLabs new anti-spam service as YKScan AS. It promises to lead the anti-spam market with success rates of over 95%. Spam is now fast becoming a major headache for HK business, greatly impacting on business' bottom lines, with employee time, bandwidth and storage space all compromised.

According to new Anglo-American research conducted on behalf of MessageLabs, one in three US emails contains spam compared to one in seven in the UK. Hong Kong is not avoiding this global trend. The research also shows the problem of spam is here to stay, with only a third of UK email users describing spam as no problem now, and three quarters of respondents predicting that it will be a 'much' or 'somewhat' bigger problem in the year ahead.

Unlike with email viruses, firms have difficulty determining what is and isn't spam leading to an 'all or nothing' approach to its prevention that fails to recognise the varying interests and needs of recipients. Indeed, nearly half of those questioned who had current spam filtering technology in place said that it was 'ineffective' or 'very ineffective'.

To combat the spam problem, and offer firms a method of detection which is flexible, intelligent and does not rely on exact match lists, MessageLabs has applied the same market

leading technology it uses on viruses to identify spam at the internet level, before it reaches the customer's system.

YKScan AS goes beyond the blacklist/whitelist filtering approach, which only picks up spam from known spammers. Instead it uses 'heuristics' scanning to build an ever-expanding knowledge base of spam techniques and behaviour to proactively identify spam no matter what its origin.

The heuristics method works by scoring each email against a set of rules. If the message achieves more than a specified score it is instantly identified as spam and the customer can choose from the tag and block options available. Businesses are therefore able to control what email does and does not get through.

Contact us at info@yuikee.com.hk for further details and pricing.

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2555 0209 Fax: 28736164
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/computer/


One Stop Anti-virus
&
Information
Security Partner
- Anti-Virus
- Firewall
- Communication Encryption
- File & Folder Encryption
- VPN
- Smartcard Token
- Content Security
- Security Check Services:
Vulnerability Scanning,
Penetration Test,
Risk Assessment ...etc.
YUI KEE