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

Yui Kee Computing Ltd.

Newsletter

December 2001

Contents

Incident Update: Goner Misses Hong Kong

W32.Goner.A@mm is a mass-mailing worm that spreads via Microsoft Outlook and ICQ file transfers. The worm arrives with the following email message:

> Subject: Hi
>
> Body: How are you ?
>
> When I saw this screen saver, I immediately thought about you I am in a harry, I promise you will love it!
>
> Attachment: GONE.SCR

Of course, the attachment is a copy of the worm, if it is opened it will send itself to addresses in the victim's Outlook address book, spread via ICQ, and delete various anti-virus and personal firewall applications.

It started spreading on the 4th December, peaking early on the 5th, HK time. By the 7th, it had all but died out. Although it was, for a short time, the commonest virus or worm, there were very few reports in Hong Kong and Asia generally. The USA and Europe were the hardest hit. The pattern of spread raises as many questions as it answers: Does it indicate that many people in Europe and the USA are regularly distributing screensavers, and, therefore, they did not see the message as suspicious? Is security awareness actually better among users in Asia? Why did the numbers drop so quickly, while other worms, such as Sircam and Badtrans, continue spreading at high levels for months?

Four high school students were arrested in Israel on the 7th December for involvement in writing and distributing W32/Goner.A@mm. They could face between three and five years in jail if convicted.

Penetration Testing

Richard Stagg, Managing Consultant, IRM (Asia) Ltd, richard.stagg@irmplc.com

It's pretty much a given, in these enlightened times, that if you run a network with any kind of permanent Internet connection, whether it's broadband or leased-line, you will need to have the security tested. After all, nothing is safe any more. Web servers are hacked and pages defaced regularly; systems are compromised, and then used to send bulk-email, or flood innocent systems with service-denying volumes of traffic. Of course, if that happens you get the blame.

For this reason, testing your network is a very important task, and one which is regularly passed on to external companies who claim to be "experts" in this field, and who use racy terms like "tiger team" to describe their "ethical hackers". But do these companies really know what they are doing? Are their testing practices actually good value for money? Critically, if they say you are secure, are you *really* secure?

The first thing that you need to understand is what they are actually selling. The term commonly used for this kind of testing work is a "penetration test". What this translates into, however, varies from company to company. In a distressingly large number of cases, buying a "penetration test" results in nothing more than being automatically scanned by a security auditing tool such as ISS's *Internet Security Scanner*, or the open-source *Nessus*. Some companies will perform a simulated attack, using commercial vulnerability testing tools such as CSC's *HEAT*.

But what does this achieve? Is this good enough? The problem is usually that the security testing companies don't sit down with the client to help them identify their real requirements. The question, you see, isn't "am I secure?"; it's "am I secure against…?" And it is this blank space that has to be filled in before any kind of testing can take place. For example, a company with a simple brochureware website need only be afraid of having it defaced – so their nemesis is the "script kiddy" hacker, who form 90% or more of the active hackers on line, but only 20% or so of the real threat. Conversely, an on-line store holding credit card numbers provides much more motivation, so their risk assessment must include the last 10% of highly skilled attackers.

The risk assessment, in an ideal world, should dictate the nature of the penetration test, or simulated attack. Sadly, too many organizations are using automated scanners which simply do not allow for these shades of detail.

Ideally, a penetration test should accurately mimic the threat identified by the risk assessment. After all, if you invited someone to mimic an intruder breaking into your office, you'd be upset if he landed a helicopter on the roof and walked in from upstairs – especially if he then charged you for the rental of the helicopter. In theory, it's a way in, but it's not a valid test of the *genuine* threats posed by real intruders. Simulated hacking attacks are no different – and since hackers do not use automated vulnerability assessment tools (for a start, they can't afford them), any penetration test that includes them should be viewed with deep suspicion.

The challenge, when arranging a penetration test, is to find an organization whose technicians not only understand exactly how hackers think, but also exactly how they go about their attacks; whose technicians perform their attacks in *exactly* the same way, using the same tools, responding identically to the same stimuli. The even greater challenge to find an organization whose technicians can do all this, and at the same time keep sufficient professional distance that they can produce meaningful results for you at the end. The greatest challenge of all is to find an organization that does all this, and is demonstrably trustworthy.

Editor's Note: Yui Kee can provide a full range of Penetration Test Services, please contact us (cdsales@yuikee.com.hk) for details.

FBI Spy Software: "Magic Lantern"

Recent news stories report that the FBI is developing software that could be installed remotely to monitor and log when suspects key in passwords for programs such as PGP. For a controversial twist, some rumours suggested that anti-virus companies were being asked to not detect the tool.

Although assisting properly-authorised law enforcement to monitor suspects might sound like a good idea the danger is that the same (or modified) spying software could be used by criminals too. Symantec, Network Associates, Trend and Sophos have all made statements denying they would put customers at risk in this way.

Don't Read this Newsletter…

Not reading this newsletter can help you detect a virus or worm on your computer. How? Some malware will search your unread messages and reply to the sender, attaching themselves. Therefore, if you leave this message unread, an infected message will be sent to Allan Dyer, who will send a warning back. Exactly this happened to one of our subscribers, whose machine was infected with W32/Badtrans.B.

Unfortunately, this is not a reliable, or foolproof method. Other viruses avoid unread messages, and send themselves to address book entries, or addresses found in the Internet cache, or a hundred other alternatives. It is better to follow the SafeHex Guidelines and keep your machine clean, instead.

Thirty Nations Sign Cybercrime Treaty

Albania, Armenia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Japan, Moldova, the Netherlands, Norway, Poland, Portugal, Romania, South Africa, Spain, Sweden, Switzerland, "the Former Yugoslav Republic of Macedonia," Ukraine, United Kingdom and the United States of America signed the Council of Europe's "Convention on Cybercrime" on 23 November. The treaty seeks to harmonise laws and penalties for crimes committed via the Internet.

A copy of the treaty is at: http://conventions.coe.int/Treaty/EN/cadreprincipal.htm

Field Experience

An interview with Johnny Cheng, one of Yui Kee's Anti-Virus Experts about a typical on-site support case.

Yui Kee Newsletter (YKN): What sort of company was this?

Johnny Cheng (JC): They are an electrical products manufacturing company, with a small office in Hong Kong (about 19 workstations and 3 servers) and a larger site in China.

YKN: Why did they need the service?

JC: They did not have any IT staff in Hong Kong. They were using a general Systems Integrator for IT support, but the SI was not up-to-speed on viruses. The company wanted a more professional service.

YKN: How did the situation develop?

JC: The Company started getting complaints from their worldwide customers that they were sending infected email. They called the SI for help and the SI cleaned up the server. However, the infections did not stop. They installed a scanner on their Exchange Server, and found a lot of W32/Badtrans.B. Really, the SI was unable to deal with the overall problem.

YKN: What viruses and worms were there?

JC: Quite a lot: W95/CIH.1002, W32/QAZ, W32/Hybris, W32/Magistr.A@mm, W32/Sircam@mm, W32/Klez@mm, W95/Elkerm, W32/Nimda.A, W32/Badtrans.B@mm and W97M/Class.

YKN: Why was their Anti-Virus Software not effective?

JC: Most machines had (a major AV brand) installed standalone, so that each user had to manually click for updates. One machine, which was a shared machine with a printer and OCR scanner attached, had that software installed, but it was not active. No one took care of that machine or had responsibility for it - it had the most viruses on it and it was probably the major route for spreading the viruses through the office. Another machine had a really old copy of (another major AV brand) installed, which had never been updated.

The anti-virus software was not faulty, but it will not provide good protection is it is not installed properly, and if it is never updated.

YKN: What about CIH, isn't that very destructive?

JC: Yes, on the 26th June, CIH overwrites part of the hard disk and tries to wipe the flash BIOS, causing serious data loss and a possible trip to the vendor for repair. That was on the shared machine, but it was just in a few files and not in memory. It would not activate and destroy anything as it was, but it would be an easy mistake for someone to click on it, allowing it to activate later. Someone could do that on another machine, across the network, if the applications are shared.

YKN: And Nimda?

JC: Nimda is a difficult one because it has multiple spreading mechanisms. The company had recently installed a Windows 2000 Server, but had not installed the security patches for IIS. They were OK for a week, and then Nimda infected the server.

YKN: What was the result of your service?

JC: First, I cleaned up all the viruses. In this sort of situation, where there is widespread infection, it is safest to scan all files. This is quite time-consuming, typically an hour per machine, although many machines can be scanned in parallel. Next, I updated, or installed, where necessary, the anti-virus software, making sure it was set for daily, scheduled updates of the virus definitions. Now, they all get updated automatically, during lunchtime. Overall, it took 8 hours, including solving some other minor problems the staff reported, such as intermittent hangs and printing problems.

YKN: What next?

JC: Now that their immediate problem is fixed, they are asking how they can be better protected in future. They need a better infrastructure and efficiency could be improved. At the moment, each machine is getting the updates from the vendor's site independently. It would be better to download the update once, and distribute that internally, but I didn't have time to set that up. A managed service, such as YKScan, would be very suitable for them - they do not have the IT staff on site, so it is better to outsource the protection, where possible. Of course, the anti-virus software on their workstations and servers is still their final line of defence.

In their situation, this on-site service was necessary, but it is better and cheaper if the whole problem can be avoided in future by having the proper protection in place.

Full Disclosure: part II

Microsoft has admitted that it mistakenly accused Online Solutions of publicising vulnerability in Internet Explorer before informing Microsoft of it. On the 1 November, Online Solutions discovered the hole and informed Microsoft's Security Response Center about it. Over a week later, Online Solutions issued a press release about the flaw to increase pressure on Microsoft to provide a fix. Microsoft issued a security alert, "Internet Explorer Cookie Data Can Be Exposed or Altered Through Script Injection (Q312461)" the same day, and accused Online Solutions of being irresponsible. They released a patch for it on November 14. However, by November 19 Microsoft retracted their earlier statements about Online Solutions and acknowledged they acted responsibly.

International Experts Exchange Views on Latest Computer Virus Combating Technologies

"Are mobile phones safe from viruses?" "Should virus writers be punished?" "What's China doing about computer viruses?" These were some of the major topics discussed in the Fourth Anti-Virus Asia Researchers Conference, which took place on the 3rd and 4th December in Hong Kong. More than 150 information security officials from many governments, anti-virus technology specialists, networks and system administrators and anti-virus vendors exchanged views and professional knowledge on combating viruses. AVAR Conference was co-organised by the Association of Anti-Virus Asia Researchers and the Information Security Special Interest Group of the HKCS.

AVAR 2001 Conference In Hong Kong
2001亞洲防電腦病毒研討會
4th - 5th December
AVAR 2001 Conference In Hong Kong
2001亞洲防電腦病毒研討會

Vesselin Bontchev gives the Day 1 Keynote Speech at the AVAR Conference

Vesselin Bontchev gave the first day keynote speech on the Responsibilities of the Anti-Virus Researcher. These are quite extensive, starting with meeting the technical challenges, education, co-operation, with other researchers and law enforcement, and ethical considerations.

Among the speakers on the first day was Jan Hruska, Chief Executive Officer of Sophos Anti-Virus, who brought along a thought provoking topic: Is virus writing really that bad? Dr. Hruska answered in the affirmative, and asked for frequent prosecution, but with modest penalties. He urged users to be ready to lodge complaints; the anti-virus companies and the media to release realistic damage figures; and for authorities to act swiftly without drama.

Zhang Jian speaks on the Anti-Virus situation in China

Mr. Zhang Jian, Senior Engineer at China's National Computer Virus Emergency Response Center, spoke on the progress of anti-virus works in China. He pointed out that the viruses CODERED and NIMDA have infected systems in many government departments, businesses and universities. Some of their networks had crashed, with incalculable losses.

The Response Center also carried out the first nationwide virus prevalence survey ever conducted in China this year, said Mr. Zhang. Among the 6000 computer users who took part in the interview, 73% of those asked had experience virus infection in their computers and 53% of them were hit three times or more. 43% of them experienced data loss in the virus attacks. Among those, 14% had lost all data. In China, the key media for virus to spread are floppy disks and CD-ROMs. In addition, the rapid development of Internet viruses will further worsen the problem in China.

There are about 22 millions internet-users in China at present, but according to Mr. Zhang, most of them have only basic computer and networks knowledge. This situation, he pointed out, makes it difficult for China to develop information security technology.

While computer viruses attract the bulk of the attention, other devices may also become victims of high-tech attacks. The functions of mobile phones have become more complicated than ever. As the technology improves, the threat of virus attacks also increases. Mr. Yuji Hoshizawa from Symantec Japan examined data security on the newly launched Java-enabled mobile phones.

This new technology allows mobile phones to download and store a variety of dynamic Java applications from the Internet. Mr. Hoshizawa concluded that these phones may not be as secure as some think, and that anti-virus vendors should look for ways to block potential virus outbreaks.

Robert Vibert introduced the Anti-Virus Information Exchange Network (AVIEN), a relatively new organisation that states its objectives as, "World domination, one PC at a time… ", and which requires members to have a sense of humour. AVIEN's serious purpose is to allow major anti-virus users to exchange information and provide mutual support. Representing over 3 million PCs worldwide, their message to vendors is that the vendors do not have all the answers.

Eva Chen (Right) is presented with a souvenier by Allan Dyer

Eva Chen, Chief Technical Officer of Trend Micro gave the keynote for the second day on the "Next Code for Virus Fighters". She challenged our old perceptions of the anti-virus developer as a doctor who is able to vaccinate the patient against future threats. Instead, the reality is closer to a fire fighter, who responds quickly and effectively to the latest outbreak.

Dennis Longley reminded us of a fundamental principle of security; that any security system that is unable to prevent a high impact from a low resourced attack is inadequate. The resistance of corporations to increase security budgets and address the problems has contributed to the development of the current situation of virus epidemics.

Katrin Tocheva covered the development of worms and classified them according to methods of spread, network environment and platform. She examined the criteria needed to achieve fast spreading in the different environments. Francois Paget also gave his thoughts on this hot topic.

The other speakers were also well received. Takashi Kume introduced information security policy in Japan and Masao Tatsuzaki reported on Japanese Cyber Crime. Vincent Gullotto reviewed the year. Szilard Stange covered the difficulties of safely sending virus samples between researchers. Randy Abrams described the coporate virus checking service. Igor Muttik took on the problems of accurately comparing the effectiveness of anti-virus software. David Barrett and Costin Raiu described their automated methods of virus analysis, called VIRTUE and MIRA, respectively. Gabor Szappanos covered the issues raised by the introduction of Office XP.

Each day ended with a panel discussion, the first on "Searching for Best Practice" and the second on "Look Back and Look Forwards, Technical Changes" that generated some interesting viewpoints.

Copies of the conference proceedings are available for purchase from the HKCS Office. AVAR 2002 will be held in Korea.

Who are the Idiots?

Allan Dyer

The AVAR conference featured a number of disagreements between participants, and this is a personal look at some of the issues raised. Despite the title, which derives from certain groups being called stupid or idiots, the discussions were all civilised and they often raised important points. As so often happens, Asian culture inhibited many people from participating, but their later feedback showed they appreciated the exchanges.

To name names, Vesselin Bontchev declared 97% of users to be idiots, and backed this up with statistics of people's reaction to being informed that their computer is infected. As it happened, W32/Goner.A@mm spread worldwide during the conference and, at the start of day two I commented that this confirmed Vesselin's statistics - as such a simple worm that requires the user to actively participate in their own downfall was so successful then there must be a lot of idiots out there. Dennis Longley turned this around and said that we were the idiots for not protecting the users. The users pay us, the IT industry, to provide working, reliable systems but the IT industry has failed to produce the security infrastructure to protect its own operations.

If 97% of users are idiots, then it is a waste of time and resources to educate them, however, education in various forms was a recurring theme of the conference. The Best Practice panel discussion raised the importance of user education and the banquet theme was "Anti-Virus Begins with Education". Between sessions, Randy Abrams showed a small group some of his materials for user training.

Jan Hruska's speech raised a controversial topic: the creation of new viruses by anti-virus researchers. Vesselin Bontchev is well known for his strong opposition to virus creation by anti-virus researchers, but, strangely, Jan and Vesselin reached an unexpected consensus. The issue was the handling of virus creation toolkits. Various virus writers or virus writing groups have released toolkits that make generation of new virus code as simple as point and click. The difficulty for the anti-virus developer is ensuring that their product can detect all possible viruses that could be generated from such a toolkit. A simplistic method would be to generate many viruses and design the anti-virus software to detect them. Vesselin contended that, apart from violating the taboo on virus creation, this approach was inadequate because there could be no guarantee that all possible forms were generated. Instead, the developer should comprehensively analyse the toolkit and predict the possible results of the algorithm used. Jan agreed with this, but pointed out that the developer should run the kit to produce source code to test the detection algorithms derived. Vesselin agreed that it was permissible to generate the source code, and even to compile parts, so long as care was always taken to disable the self-replicating function so that self-replicating executable code was never produced.

It was also clear that there is tension between the anti-virus developers and the users. Representing a large body of users, AVIEN presented its wish list, including a working naming standard for viruses and alternative approaches to anti-virus, including behaviour blockers and a 'whitelist' product that would only allow acceptable programs to run. The list was criticised as unrealistic and self-contradictory, for example, behaviour blocking and integrity checking products have not been commercially successful (which is another measure of user's desires) and Windows XP allows workstations to be locked down to only run approved software, but companies are not rushing to take advantage of this feature.

I think there is no One True Way of anti-virus, and we can all learn from these viewpoints to improve our strategies.

Anti-Virus Begins with Education

The banquet theme for the AVAR Conference was "Anti-Virus Begins with Education" and Karen Cheung (Organising Committee Chair and Yui Kee Computing Business Development Manager) introduced two projects.

The first one started with a story: Around a year ago. A lecturer from Chu Hai College called Yui Kee Computing to join one of their school projects, by supervising a group of part-time Information Technology students to accomplish a project, so that these students will learn from the process and they would make something useful. The students were convinced to create a web site aim at assisting young people to learn about Ethics, Safety and Security on Information Technology.

Ms Cheung and Mr. Dyer advised the students over a couple of meetings during the project and were happy to see some results.

Alex Leung, Denny Mo and Gordon Luk demonstrate their website

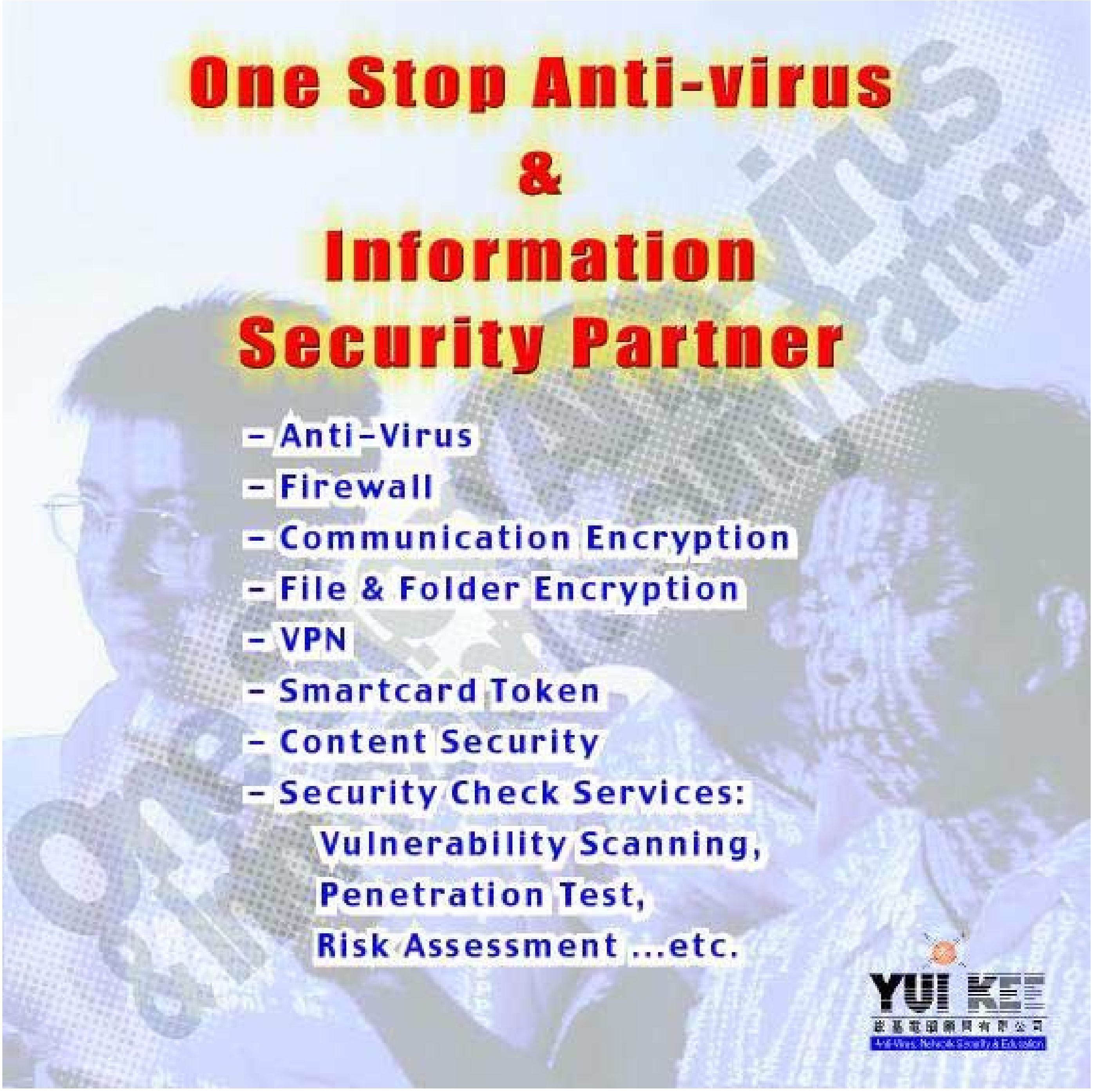
The students, Mr. Alex Leung, Denny Mo and Gordon Luk, presented their educational multimedia website and explained some of the ideas behind the design. It is a fresh, fun approach, by young people, for young people.

Alex, Denny and Gordon started a candle-lighting ceremony, passing light to each table as Karen with the metaphor of “It is better to light a candle than to curse the darkness” explained that, in the journey of Anti-virus, we see new viruses coming out everyday, created by people whom have the computing skills but not the computing ethics and, to build a bigger force of Anti-virus and awareness of information security, we rely on Education in all forms and all directions. She invited everyone to take the idea back to their country to share with educators and learners, and build up many more different learning resource sites, with young people around the world. Perhaps in less than a year’s time, we’ll have Japanese, Indian, Icelandic, Korean, Czech - multiple language learning kits that AVAR can gather together in cyberspace.

The student's project is included on the Conference CD-ROM in Chinese and English, and is currently at http://www.anti-virus.com.hk/

The second project under the Anti-Virus Beings with Education theme was a starting point - Mr. Dyer announced that the Hong Kong Chapter of AVAR would be starting a project to develop an international standard for certification of anti-virus professionals, and said he would be seeking support and assistance for the project.

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.