Yui Kee Computing Ltd.

Newsletter

May 2001

Contents

Anti-Virus Licensing

Following the introduction of new Copyright laws in Hong Kong it is appropriate to clear-up confusion about licensing of Anti-Virus software.

It is not possible to generalise very much - each developer has their own licensing terms, and even the terminology used varies considerably. Here we will talk about Updates and Upgrades. For the purposes of this article, an Update is a package of virus definitions, without any change to the basic functionality of the product - these may be referred to as "virus signatures", or "virus identity files (IDE)" etc. An Upgrade includes change(s) to the basic functionality of the product, it may be indicated by a change to the version number (e.g. 1.01 to 1.02), and this may include bug fixes or extra functions. Note that an Upgrade may have a large effect on the ability to catch viruses, for example, Bubbleboy was a virus that infected the body of email messages, a product that did not search email message bodies could not find it, even if it had an Update that included the recognition - an Upgrade that included "Scan email message bodies" functionality was also required.

One commonality is that the license will have a "size" - number of users, number of servers, gateways etc. Organisations should take care not to exceed any of these limits - enlarging a license is quite simple.

F-Secure

The initial purchase includes one-year "support and maintenance service", i.e. Upgrades and Updates, which can be renewed thereafter. If the "support and maintenance service" period expires, the user has the right to use the last Updates and Upgrades received (obviously, risking infection by a new virus). Because the infection risk is significant, F-Secure strongly recommends its' customers to have the ongoing support and maintenance service and also install the products updates on regular basis.

Symantec

The Symantec license is a perpetual license. Symantec Antivirus licenses include one year Updates and Upgrades. Users can then purchase Upgrade Insurance in order to continue

enjoying the maintenance. During the maintenance period, users receive major Upgrades (e.g., 8.0 to 9.0) on CD and can download minor Upgrades (e.g. 8.0 to 8.1) and Updates from the Symantec site.

Sophos

Sophos Anti-Virus is sold on a subscription basis; therefore users are not entitled to use the software after their subscription expires. The initial license price includes the first-year subscription, which can be renewed thereafter. Multi-year licenses are available at a discount.

Disclaimer

While we believe these to be a fair and accurate summary of the licensing terms for the anti-virus products of these companies we cannot guarantee their accuracy, or that they have not changed since our research or the possibility that other details in the licenses do not change your situation. Please confirm your position with the developer(s) concerned.

Yui Kee Computing Ltd. Renewed as F-Secure Authorized Distributor

Karen Cheung (Business Development Manager, Yui Kee Computing Ltd.) shakes on the agreement with Mika Kolbe (Vice President Sales - Asia Pacific, F-Secure Corporation)

We are pleased to announce the renewal of our partnership with F-Secure Corporation, a leading Finnish Data Security and Anti-virus developer.

Yui Kee Computing is a Certified F-Secure Anti-Virus Centre in Asia and houses Certified F-Secure Framework experts and Anti-virus experts. Since it's commencement in 1993, Yui Kee has gained great trust and confidence of an extensive clientele and partners. Yui Kee's top management are founding members of the Association of anti-Virus Asian Researchers (AVAR) and advisory committee member of the newly established Hong Kong Computer Emergency Response Team (HKCERT).

Yui Kee Computing is committed to take on an independent and professional stance in providing our clients with all round protection with the best bred of products, services and advice in the Information Security field.

SadMind Exploits Old Vulnerabilities

SadMind is a worm that spreads on Solaris systems. Additionally, it breaks into Microsoft IIS servers and replaces the homepage with an obscene message. Possibly hundreds of websites have been defaced by this worm since the beginning of May, but this could have been avoided.

SadMind infects Solaris systems by taking advantage of a two-year old buffer overflow vulnerability. It breaks into the IIS servers using a seven-month old directory traversal vulnerability. It would not have spread if Solaris administrators had installed the patch during the past two years. It could not have defaced the webpages if IIS administrators had installed the patch during the past seven months.

Lesson to learn: Keep up-to-date: **Install the Security Patches**.

For further information and the relevant patches see:

http://www.cert.org/advisories/CA-2001-11.html

http://www.sophos.com/virusinfo/analyses/unixsadmind.html

http://www.sarc.com/avcenter/venc/data/backdoor.sadmind.html

http://www.f-secure.com/v-descs/sadmind.shtml

http://www.symantec.com/press/2001/n010514a.html

YKScan powered by MessageLabs shows its mettle

May has been the busiest month ever for the MessageLabs' Global Network that powers YKScan. More than 77,000 viruses have been stopped so far, paling the previous high of 46,291 viruses stopped in February. The culprits included two viruses never seen before and the re-appearance of w32/Magistr-mm, which originally broke out of Spain back in March and has now hit 136 countries. The new viruses were the now well-publicised Homepage and VBS/Mawanella.A-mm - a worm emanating from Sri Lanka.

Homepage was by far the most serious, flinging more than 39,000 copies across 77 countries - with more than 4,000 going to/from Hong Kong and Taiwan. Of course, these figures are for those viruses intercepted by MessageLabs and YKScan, so our customers were not automatically directed to a Dutch porn site - unlike many thousands of other email users around the globe.

The appearance VBS/Mawanella.A-mm once again proved that the belts-and-braces approach with multiple scanning engines is vital to ensuring total protection. While Homepage was stopped by two of the four engines used, the Sri Lankan virus wormed its way through conventional defences only to run up against Skeptic. Just as in the LoveBug outbreak, Skeptic - MessageLabs' unique heuristics scanning technology used by YKScan - was the first to detect and stop a previously unknown virus.

While May has starkly shown the increasing trend of growing numbers of viruses traversing the Internet, we are happy to report that not a single one of YKScan customers was hit. MessageLabs' 100% record remains intact.

Homepage and Mawanella

These two worms received some attention when they spread around the world on the 9th and 17th of May. Technically referred to as VBS/VBSWG.X@mm and VBS/VBSWG.Z@mm, they are both based on the same worm generating kit. However, they came from different corners of the globe, Homepage from the Netherlands and Mawanella from Sri Lanka. Why did these spread successfully when many other very similar worms fail? They arrive in email and require the user to click on the attachment in order to spread further, so maybe the text of the message is critical. Alternatively, perhaps they got a "lucky break" - infecting a victim with a large address book of gullible friends, or maybe the author was persistent in sending copies to multiple addresses until the epidemic started.

However, whichever was the actual case, it was avoidable. Any one of these methods would have prevented VBS/VBSWG.X@mm or VBS/VBSWG.Z@mm from affecting an organisation:

- Uninstall the Windows Scripting Host (see http://www.sophos.com/support/faqs/wsh.html or http://www.f-secure.com/virus-info/u-vbs/)
- Delete executable (or just .VBS) attachments at your mail gateway (see http://vmyths.com/rant.cfm?id=239&page=4)
- Educate users to follow the Safe Hex guidelines (see http://www.sophos.com/virusinfo/articles/safehex.html - users)
- Use our managed email security service, YKScan (see http://web.yuikee.com.hk/computer/press/release/2001-04_MLABHK_.htm.en)

Of course, these methods will not prevent all viruses and worms with 100% certainty (e.g. viruses downloaded from the web, or on CD-ROMs) but if your organisation has just been hit by an email worm **again**, please try at least one before the next time.

The Costs of FunLove

The most publicised viruses are not necessarily the most costly. W32/FunLove (also known as W32/Flcss) is a memory-resident Win32 virus that was discovered in November 1999. However, several large organisations in Hong Kong have been affected recently and, because it spreads via network shares, once it is established at a site it is difficult to get rid of - infected machines can re-infect machines across the network faster than technicians can clean them. Disconnecting everything from the network and reconnecting machines when they have been cleaned and verified is the simplest option. Obviously, this severely disrupts the organisation and will be unpopular with users, so accomplishing it requires power and authority. Compare this with the current biological virus situation - H5N1 and the chicken slaughter, which has support from the highest levels of government.

Additionally, disinfecting machines is not trivial because the virus is memory-resident. Detailed disinfection instructions are available:

- http://www.sophos.com/support/faqs/flcss.html
- http://vil.nai.com/vil/virusRemovalInstructions.asp?virus_k=10419
- http://www.symantec.com/avcenter/venc/data/dos.funlove.4099.fix.tool.html

Finally, on NT systems, FunLove modifies the NT kernel (NTOSKRNL.EXE) and NT loader (NTLDR), disabling access control - all users can access all files. Therefore, these must be replaced from a clean source (backup or a Service Pack).

Altogether, this is a lot of work for technicians, and a lot of disruption for users. However, it is less likely to get in the news than a email worm outbreak for two reasons: Email worms are effectively self-publicising - all the contacts of the victim receive a copy, and most of their contacts, and so on, until a reporter notices and documents the infected companies. Conversely, it is easier to keep news of a FunLove outbreak inside a company. Secondly, FunLove spreads between organisations slowly, whereas email worms typically have a massive outbreak, and then almost disappear.

Different Approaches

Last month we featured Information Security Management and BS7799, but the Black Hat Briefings, which visited Hong Kong in April, focussed on the complementary approach. BS7799 concentrates on the management issues, and the Black Hat Briefings are highly technical - forensic analysis of a hacked server or web exploits via SQL will make most managers eyes glaze.

Black Hat Briefings is a wonderful opportunity for technical staff to improve their skills and gain new perspectives, and this is applies not just to security-related staff. Your development team, naturally, concentrates on getting your applications working and available, but it is their oversights that create the buffer overflow vulnerabilities and insecure configurations that hackers exploit. They could certainly benefit from the paradigm shift of seeing how obvious the flaws are, and how easily hackers exploit them (this is "obvious" as in "why didn't I think of that", but in many cases, no tools beyond a browser were required). Some tolerance of eccentric behaviour is required, the speakers were almost exclusively younger than the business-attired audience, and dressed "casual" (or perhaps "scruffy"). Some took this "information warrior at the edge of civilisation" attitude too far - was it really necessary for Rain Forest Puppy to require the organisers to sign a non-disclosure agreement before he would reveal his real name so that travel arrangements could be made? Do his friends call him Rain, and should we address him as Mr. Puppy? The important point is to see the truth behind the distractions - the vulnerabilities and exploits covered are real, and many sites on the Internet, probably including the sites many of you are responsible for, are at risk.

However, many of the technical experts at Black Hat Briefings have difficulty in practical security for real organisations. This could be seen in statements like, "users should avoid executing ..." or others implying developers are responsible for buffer overflows, or that systems administrators are to blame for not applying security patches.. This is blaming the victim for the crime. The real question for organisations is, given that we have human staff and tight schedules, how do we minimise the cost of incidents? The keynote speaker, Bruce Schneier addressed this, saying that the way forwards is to think "risk management", not "threat avoidance".

Which approach do organisations need? Both: top-level support for a clearly defined security policy and delegation to expertise in specific technical areas so that the details are addressed.

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/

AVAR 2001 Call for Papers

4th Anti-Virus Asia Researchers Conference

4 - 5 December 2001

New World Renaissance Hotel, Hong Kong

The AVAR Conference is an annual event organised by the Association of Anti-Virus Asia Researchers (AVAR) since 1998. It will provide information on how the anti-virus community works together globally, latest virus, anti-virus technology (developments), and virus status from various countries in Asia. It will be the second international anti-virus conference held in Hong Kong

The conference is co-organised by the Information Security Special Interest Group (ISSIG) of the Hong Kong Computer Society (HKCS).

We invite paper submissions that address any area related to computer viruses.

Submission of Abstracts

Prospective authors should submit the following information to the AVAR 2001 Programme Chairman, Mr. Allan Dyer at avar-papers@yuikee.com.hk no later than 15 June 2001:

1. paper title
2. author's name and affiliation
3. contact email, phone and physical addresses
4. an abstract of not more than 200 words

Submissions should be in plain-text, PDF or MS Word format. Notification of our acceptance for papers will be distributed by 15 July 2001.

Submission of Papers

Final papers should reach the HKCS Office no later than 1 October 2001. Papers should be submitted in both hardcopy and electronic form (PDF or MS Word). All illustrations should be camera ready.

Presentation of Papers

Paper presentations must **not** exceed 40 minutes including 5 minutes for questions. Speakers should indicate their audio-visual and computing equipment requirements for presentation of papers.

Official Language

The official language of the conference is English. Chinese translation will be supported.

Exempted from Registration Fee

The speakers are exempted from the normal registration fee and are entitled to attend all sessions of the two-day conference, lunch on 4 - 5 December and banquet on 4 December.