Yui Kee Computing Ltd.

Newsletter

April 2002

Contents

Editors Notes

Another month, another virus outbreak, W32/Klez.H is the current threat. We also have news about user education and the ICDL, opinion on the ETO review and other news items.

Incident Update

W32/Klez.H@mm, the latest mass-mailing computer virus sometimes tries to trick users into launching it by saying it is a cure for an earlier variant of the same virus. The virus emails itself to addresses found in the Windows address book, the ICQ database, and local files, using another such address as the From: field. Thus, when you receive W32/Klez.H, the apparent sender may not be infected. The SMTP envelope From: address (usually seen in the headers as the Return-path:) will probably give a more accurate indication of the source.

However, it may not need the users' assistance to spread: it uses a known vulnerability in Internet Explorer-based email clients in order to execute automatically. The vulnerability is known as Automatic Execution of Embedded MIME type and all users of Microsoft email clients should make sure they have the relevant patch installed, see the Microsoft Security Bulletin:

http://www.microsoft.com/technet/security/bulletin/ms01-020.asp

It is also capable of spreading across a LAN by copying itself to shared drives or folders. This can make it difficult to eradicate in large networks with few internal controls.

Some anti-virus products are able to detect the new variant because of its' similarity with previous variants: Sophos Anti-Virus detect it with their 7 February definition file for W32/Klez.G and McAfee detect it as W32/Klez.gen@mm with their 23 January definition file (4182 DATs).

MessageLabs first stopped W32/Klez.K-mm in an email from China on 15th April, but did not see another copy until 17th April. To date, they have seen the most copies from the UK, with Hong Kong in third place, only marginally behind the USA. Given the relative size of these places, this indicates a distressingly high prevalence in Hong Kong.

Allan Dyer, Chief Consultant of Yui Kee Computing, commented, "Outbreaks like this are becoming commoner and the ability of organisations to cope with them depend on good user education, preparation of their defences and incident response planning." A good starting point for user education are the Safe Hex Guidelines:

http://www.sophos.com/virusinfo/articles/safehex.html

More Information

Sophos Anti-Virus: http://www.sophos.com/virusinfo/articles/klezh.html
MessageLabs: http://www.messagelabs.com/
Computer Associates: http://www3.ca.com/virus/virus.asp?ID=11779
Trend Micro:
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=WORM_KLEZ.G&VSect=T
McAfee: http://vil.nai.com/vil/content/v_99455.htm
Symantec: http://www.sarc.com/avcenter/venc/data/w32.klez.h@mm.html
F-Secure: http://www.f-secure.com/v-descs/klez_h.shtml
Norman: http://www.norman.com/virus_info/w32_klez_g_mm.shtml
Hongkong Cert: http://www.hongkongcert.org/valert/content.html
HK Government, ITSD: http://www.itsd.gov.hk/itsd/virus/alert/alerts.htm

Timely Warnings

Anti-virus developers and CERT organisations rush to publish information on the latest virus threats on their websites, but how often do you check those sites? Could you take useful action if you received an alert earlier? Was the first you heard of W32/Klez.H from a user, "I clicked on this and something happened", or worse your boss, "What are we doing about this new virus?"

Yui Kee has developed its' own website monitoring software to address this problem. Currently configured to monitor nine major anti-virus websites, it picks out the latest virus information from each and composes a short email when it recognises a significant change. The email is suitable for directing to a pager or mobile phone, and it only contains the site, the virus name and an indication of the severity. However, this is sufficient for an Information Security Manager to understand the basic situation, and know where to get more details. Thus alerted, the IS Manager can take a variety of actions: start downloading the new update, reconfigure the incoming email filters, send a warning email to staff, etc.

Why monitor so many sites? The site that has the first alert for one virus might be last for another, and some sites are more prone to inflating the severity rating they assign, so multiple alerts are a backup and confirm the importance.

For more details of this service, please contact Lois So: lois@yuikee.com.hk or complete and return the form:

YKAlert Service Trial

Please subscribe this email address for a 14-day free trial of the YKAlert Service:

Name:
Organisation:
Email Address:

Subscribe

What to Scan?

Even if your anti-virus software is capable of detecting a particular virus, it might not succeed, at least, not in all circumstances. It depends on what it is configured to scan, and that is a trade-off between speed and security. Many types of file cannot harbour an active virus, such as JPEG or GIF images, or plain, ASCII text. Opening a file, and examining the contents to determine the type is time-consuming. It is much faster to simply rely on the filename, if a file has a `.jpg` extension, then it is never going to get executed, and therefore there is no point in scanning it.

Thus, anti-virus software usually has a list of file extensions that are scanned. The default list is usually reasonable, but sometimes it will not reflect the changing circumstances in the real world. We have seen this recently, with one anti-virus software missing some instances of W32/Klez.H@mm because it did not scan `.bat` files by default. There will usually also be an option for "scan all files".

Our recommendation is:

1. If possible, select "scan all files" - this is the safest, but many users will find the speed reduction intolerable.
2. Set a minimum of these extensions to be scanned:

no extension	DRV	MPP	SHB
386	EML	MPT	SHS
3GR	EXE	MSG	SRC
ACM	FLT	MSO	SWE
ADD	FON	NWS	SYS
ASD	FOT	OBD	TD0
ASP	HLP	OBT	TLB
AX	HT?	OCX	TSP
BAT	HTA	OV?	TT6
BIN	HTML	PCI	VB?
BOO	HTT	PDF	VWP
CHM	I13	PDR	VXD
CMD	IFS	PIF	WBK
CNV	INF	PL	WBT
COM	INI	POT	WIZ
CPL	JS	PP?	WML
CSC	JSE	PRC	WPC
DBX	LNK	PWZ	WSC
DLL	MDB	RTF	WSH
DMD	MOD	SCR	XL?
DO?	MPD	SH	

3. If an outbreak occurs, scan all files on affected systems.

Security Surveys

In March, the International Computer Security Association (ICSA) Labs released its' 7th Annual Virus Prevalence Survey. Based on data from 300 companies and US government agencies, it shows that the rate of malicious code infection continues to rise, despite increased spending on protection measures. For details see:

http://www.trusecure.com/html/news/press/2002/pravsurvey030402.shtml

On 7th April, the Computer Security Institute announced the results of their annual survey of 503 computer security practitioners in US organisations. The comparisons with previous years

are interesting, in many cases, such as for the Security Technologies Used, Likely Sources of Attack and Types of Attach or Misuse Detected, the differences are small and, given the small sample size, probably less than the sampling error. The total annual losses that could be quantified reported continued to grow, reaching US$455 million. For details see:

http://www.gocsi.com/press/20020407.html

Computer Driving Licence Popularity Rises

User Education is important throughout IT, and the International Computer Driving License (ICDL) aims to establish a benchmark of basic IT skills. The European Computer Driving License is the form of the ICDL adopted within the European Union.

The UK National Health Service has made the ECDL a standard for its entire 700,000 staff. The initiative is aimed at empowering everyone from porters to senior medical consultants with IT skills. It is also being linked to another NHS project, Clinician Connect, which will give computer and Internet access to all clinical staff. The British Computer Society, which oversees the ECDL says that basic IT skills standards must be achieved if the Clinician Connect project is to succeed. Well over 300,000 people in the UK have gained or started working for the ECDL since its launch in May 1998 and the Egyptian Ministry of Higher Education has also endorsed the ICDL.

The ICDL is operated by the IT Training Quality & Certification Institute (ITTQC) in Hong Kong. More information:

http://www.ittqc.com/

http://www.ecdl.co.uk/

New F-Secure Distributor

After a relationship of almost 9 years, Yui Kee is ceasing distribution of F-Secure products, effective from 19th April. Since their IPO in November 1999, F-Secure has been more influenced by fickle market pressure. F-Secure has closed their offices in Hong Kong and China. More recently, they have concentrated on solutions for highly fashionable mobile devices, although only one unimportant virus exists for PalmOS. Although the core scanner technology is excellent, avoidable errors have led to a reduction of effectiveness, for example not scanning .BAT and .LNK files risks missing W32/SirCam.A, which is in the Wild. This led to F-Secure Anti-Virus 5.30.7262 for Windows ME failing to get the Virus Bulletin 100% Award in February 2002.

Technical Support for F-Secure products will now be provided by the new distributor, Computech Holdings Limited: Mr. Ralph Wu Tel: 2157 8883; Fax: 2811 8892; ralph.wu@computech.com.hk. Yui Kee will still try to assist whenever possible - we remain a one-stop professional security integrator that will exercise our best knowledge and experience to recommend solutions that fit your needs.

Does Microsoft Understand Security?

January's Newsletter discussed Microsoft's new focus on security, but a recent interview of Paul Flessner, senior vice president of Microsoft Corp.'s .Net Enterprise Server group by ComputerWorld (http://www.idg.com.hk/cw/readstory.asp?aid=20020416003) casts doubt on the company's sincerity, or their ability, to achieve "Trustworthy Computing". At one point Flessner says, "I think our security model is very sound", which begs the question: Then why do they need this massive change of direction at all?

Flessner talks at length about how much effort they are putting in to code review, which is necessary remedial action, but will they recognise and admit the major security design flaws? Where is the announcement that the next release of Outlook Express will not support scripting? How about making macro support in Office applications optional, not installed by default? These are a couple of the major contributors to insecurity, stemming from breaking the rule that Code and Data should not be mixed. In January's memo, Bill Gates said, "when we face a choice between adding features and resolving security issues, we need to choose security", will they bite the bullet and remove the features that currently contribute so much to security problems?

Review of the Electronic Transactions Ordinance

The Electronic Transactions Ordinance (ETO) was enacted in Hong Kong on 5 January 2000 and came into force in April 2000. As this is a fast-changing field, the Information Technology and Broadcasting Bureau (ITBB) is conducting a review and is now invite public views on their proposals as well as comments on any other aspects of the ETO. The public consultation document is available at:

http://www.info.gov.hk/itbb/english/paper/doc/ETOreview-Consultation(E).doc

Comments should be sent to the ITBB by 30 April 2002.

In the interests of promoting open debate on this important legislation, Allan Dyer offers some comments:

One of the suggestions is considering whether legal recognition should be extended to cover other forms of electronic signatures, in addition to digital signature, in order to stimulate e-business development. In the ETO, an electronic signature is any symbols adopted for the purpose of authenticating or approving an electronic record, and a digital signature is a subset of electronic signature that uses an asymmetric cryptosystem and a hash function I consider that extending legal recognition to any forms of electronic signature that are less robustly secure than digital signatures would be a step backwards and would discourage e-business development. Digital signatures offer a high level of integrity, authentication and non-repudiation that other current technologies cannot match. Increasing computing power has made digital signatures feasible on most current computing platforms; in the near future even small handheld devices will be able to perform digital signing in an acceptable time. Security fears are often cited for reluctance to adopt e-business. New technologies "take off" when a critical mass is reached. Recognition of other type of electronic signature would merely reduce the security and fragment the market, with a negative effect on e-business development. A major advantage of Digital Signatures is that a single Private Key can be used for signing everything - once a user has enrolled and got their Certificate for one purpose, they can use it for every other service that supports Digital Signatures without further enrolment. Thus, once a person starts using a Digital Signature, they will want to use it for everything, and the effect snowballs.

This is not to say that the ITBB should not consider new technologies in future, just that offering a "choice" of using older, weaker, more flawed technologies will not encourage e-business development. Digital Signatures are the best available technology for electronic signatures today, and there is no reason to encourage adoption of less suitable systems.

Connected with the consideration of weaker forms of authentication, the ITBB recommends, "We, therefore, consider that there is a case for the ETO to be

amended and a new schedule added so that the Secretary for Information Technology and Broadcasting (the Secretary) may, by subsidiary legislation, specify in the new schedule legal provisions under which the use of PIN will be accepted for satisfying the signature requirement." Specifically citing the Electronic Service Delivery Scheme as a case where there is already established relationship between the parties involved and strong encryption services for data transmission are used, thus making the level of security commensurate with the risk of the service involved. However, although ESD booths may be secure in themselves, most people nowadays are suffering from "PIN/password overload" and, in a misguided effort to cope, are re-using passwords in different security domains (i.e., using the same password whenever they are required to choose one). Thus, an attacker could harvest passwords from an insecure online service (or might be the legitimate owner of a website using passwords), and then attempt to use those passwords at ESD booths with a reasonable proportion of successes. This is an interesting example of the weakest link determining the overall security - although the booths are secure, the user's management of their multiple passwords is flawed, making the system vulnerable.

Of course, Digital Signatures are not susceptible to this weakness - even though the same key-pair is used in both situations, the attacker cannot get the private key necessary for beating the authentication at the ESD booths. In fact, Digital Signatures offer an escape from "password overload", which is an excellent reason for promoting their widespread use.

One of the applications where the ITBB suggests a PIN might be suitable is for Tax Return submission, but there is no evidence that a PIN option would encourage more electronic submissions. I did not use my eCert to sign and submit my tax return because I could not make a joint submission, changing to a password scheme would not help this.

The ITBB also looked at biometrics and concluded, "We, therefore, consider that other means of authentication including biometrics should be examined at a later stage when they become more mature, and when related institutional support emerges in the market." Biometrics are an excellent means of authentication where there is a trusted reader, which makes them generally unsuitable for e-business, I discussed this at greater length in an earlier issue of this newsletter:

http://www.yuikee.com.hk/computer/info-ctr/newsletter/ykcl-news01-02.pdf

I see that the key enabler that legislation can provide to encourage greater adoption of e-Commerce is a secure standard. A confusion of stronger and weaker electronic signature options will merely fragment the marketplace, and confuse consumers. This can be compared to cash - the Government sets the standard, and traders decide on whether they have a till, or a vending machine or whatever.

Allan Dyer

Apache vs IIS

A recent article in eWeek said, "Enterprises last week had 11 more reasons to rethink using IIS: 10 new security holes in the Microsoft Web server and the arrival of Apache 2.0."

Now that a version of Apache that was built for Windows is available, it is difficult to see why any organisation that values there website persists in using IIS.

For details see: http://www.eweek.com/article/0,3658,s=702&a=25458,00.asp

Lawyers sue Spammers

Spam constitutes a Denial of Service Attack for many people nowadays; just clicking "Delete" for the messages takes valuable time. There is also the cost of other resources used - bandwidth probably being the most significant, but maintaining sufficient disk space on server so that legitimate email is never rejected is also a consideration. A San Francisco Law firm has decided to sue a e-mail marketing firm called Etracks for damages of US$50 per email.

For details see: http://news.bbc.co.uk/hi/english/sci/tech/newsid_1917000/1917458.stm

Sophos Awarded Two Queen's Awards for Enterprise

Oxfordshire anti-virus developer praised for exceptional innovation and international trade.

Sophos has been awarded two prestigious Queen's Awards for Enterprise on 21st April, 2002, the UK's top awards for business performance. The Oxfordshire-based company has been rewarded for both its technical excellence and business acumen by receiving awards in two separate categories - 'Innovation' and 'International Trade'.

In the category of International Trade, the Queen's Award for Enterprise has been awarded for Sophos's outstanding achievement in increasing overseas earnings. During the past three years, the company's earnings from international trade have increased by 168 percent to more than £11 million. The judges also praised Sophos's successful establishment of subsidiary companies in the USA, Germany, Australia, France, Singapore, Italy and Japan.

In the category of Innovation, the judges chose Sophos for its achievement in continuously developing and updating anti-virus software specifically designed to protect business networks from malicious attack.

This double achievement follows an outstanding year for Sophos. During the period ending March 2001, Sophos's turnover grew 54 percent, more than double the average anti-virus industry growth rate[1]. In December 2001, Sophos was also named Company of the Year at the CBI's annual Growing Business Awards. Continuing this growth, the company is currently constructing a new £32 million high-security research and development centre at its headquarters in Abingdon.

The award winners have been announced to mark Her Majesty The Queen's birthday. Sophos's two awards will be formally conferred later in the year and representatives of the company have been invited to attend a reception at the Department of Trade Industry (DTI) in the presence of His Royal Highness The Duke of York.

Sophos in Hong Kong

Sophos is represented and supported by Yui Kee Computing Ltd in Hong Kong. Within the short time since its landing in this region, it has gained trust from major corporations including the Hong Kong Jockey Club, The University of Science and Technology, and Hong Kong and Shanghai Banking Corporation. Sophos solutions are specifically designed to protect businesses and organisations from virus attack; they are widely deployed by large corporations, banks and governments.

"We appreciate Sophos philosophy in valuing each virus and each update. They are one of the few anti-virus developers that support a wide range of platforms even though those platforms are not so common, such as OpenVMS and OS/2." Karen Cheung - Business Development Manager

[1] IDC Research's "Worldwide Anti-virus Software Market Forecast and Analysis, 2001-2005" estimated the anti-virus industry grew at 24% for the period 1999/2000.

For a free trial and a quote, please contact: 28708553 / lois@yuikee.com.hk

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/