
**Yui Kee Computing Ltd.**

# Newsletter

May 2002

## Contents



## Incident Update

W32/Klez is still dominating the current incidents and it is unlikely to die out soon for two reasons: First, it generates email with a wide variety of different subjects, so recognition is difficult. Second, it forges the From: header, so that recipients who recognise it and take the trouble to warn the apparent sender are telling the wrong person. Thus, the victim with an infected machine keeps sending out infected messages and is never told. Actually, it is inaccurate to say recognition is difficult - W32/Klez can be easily detected by up-to-date anti-virus software, so, it is now a minor threat for all sensible computer users, but a continuing annoyance as we receive infected emails from the dumb computer users.

## 'JDBGMGR' causing net confusion

**Sophos says don't be duped by hoax**

Sophos has issued a warning about the latest hoax message about a 'virus' sweeping the internet. Sophos has already received enquiries from thousands of concerned computer users.

The fake warning tells users to search their hard drives for a file called JDBGMGR.EXE. The message also advises users to delete the file because it is infected by a virus which may trigger after 14 days.

But JDBGMGR.EXE is the Microsoft Debugger Registrar for Java and may be present quite legitimately on many computers.

The confusion is compounded by the W32/Magistr-A virus, which is capable of emailing infected copies of JDBGMGR.EXE to innocent users. Most anti-virus software has been capable of detecting W32/Magistr-A for over a year.

"If you receive an unsolicited executable file in your email, simply delete the email," said Graham Cluley, senior technology consultant at Sophos Anti-Virus. "This is a confusing hoax, but the message is simple: you should never launch or open unsolicited code on you computer. The best way to check for a virus infection is with anti-virus software. If your anti-virus software is up to date, you will be protected from the Magistr virus anyway."

Sophos reminds users that they should not pass on virus warnings to friends. Instead, check the facts at an anti-virus website, or forward the warning to the person in your company who is responsible for virus protection so they can decide if it is valid.

Sophos offers a free hoax information feed, which enables webmasters to place "always fresh" data about the latest internet myths, as well as real virus threats, on their public websites and company intranets. For more information, and to quickly add the feature to your website or intranet please visit: http://www.sophos.com/virusinfo/infofeed/

Sophos has published advice on this hoax at:

http://www.sophos.com/virusinfo/hoaxes/jdbgmgr.html

More information about Magistr-A is available at:

http://www.sophos.com/virusinfo/analyses/w32mag.html

# "War Carding"

A recent report (see: http://www.msnbc.com/news/742677.asp) describes how criminals are using an Internet payment gateway to check for valid credit card numbers. The criminals use a stolen merchant's account to check thousands of random card numbers, and the merchant is charged for each failed transaction. Presumably, the criminals then run up substantial charges on the tiny percentage of card numbers that got validated.

The major weakness here is that the merchant accounts are only secured with a user name and password, or sometime even only a password, making it easy for criminals to get access. Merchants are blaming the payment gateway company.

There is a lesson here for the review of the Electronic Transactions Ordinance: if there is a weak (and easy) authentication option, people will want to use it, demand to use it, will use it, even when it is inappropriate.

# No More Global Village

*Natasha Staley, Sophos Plc*

A growing reliance on the Internet as a business tool has seen the web grow from being a small village - where all users knew and trusted each other - to a sprawling metropolis. Much like a real city, this growth has brought more choice and diversity, but it has also heralded more dangers. The internet now has its own 'no go' areas complete with bad guys.

However - again much like the real world - there is a difference between real and perceived threats. Reading many IT security vendors' promotional material is enough to make a financial company think twice about incorporating any internet communications into their critical business systems. But, in today's connected age, this option is as unrealistic as not crossing the road for fear of being knocked over by a bus. With internet banking, email communications and networked computing integral to all financial institutions' business activities, it is time to debunk the security hype and look at the real threats, their costs and solutions.

Virus writers in particular have been taken advantage of the ubiquity of the Internet. There are currently more than 73,000 viruses in existence; this figure is rising by between 500 and 1,000 each month. The typical virus writer is a single man in his teens or twenties, often with a chip on his shoulder about society at large. Banks and other institutions, which are perceived to represent the 'evils' of capitalism, are a prime target for these virus writers. In addition, because viruses can spread without the sender actually being aware of their actions, institutions are just as likely to receive an unprovoked attack from their customers, colleagues and business partners.

That said, only 3 percent of these viruses are actually circulating in the wild and fewer still have had the impact of the Love Bug, Anna Kournikova or the current most prevalent worm, Klez-H. However, those that do hit are capable of doing considerable damage. It is impossible to pinpoint the exact monetary cost of infection, but by looking at the cost of network downtime, the amount of data lost or damaged and the negative impact on corporate reputation, it becomes apparent that multi-level virus protection is both necessary and cost-effective.

Viruses are not just about inconveniencing computer users; some delete files, corrupt data or modify hard disks. The more high profile infections have come from email aware viruses, which have forced companies to shut down their email servers and vital systems, simply because of the volume of email created.

The most 'successful' pieces of malware are those which do not deliberately make their presence known. These viruses, which sit quietly in the background, forwarding themselves or subtly corrupting data, can often remain undetected for weeks or even months.

For the financial community, the most damaging type of virus is often the 'data diddler'. This code will surreptitiously modify the data within a spreadsheet, perhaps multiplying cells D4 and F8 by 1.001 on the first Monday of the month. The chances are that it will be some time before anyone notices that the figures have changed. By this time the likelihood is that back ups will also be corrupted. Unauthorised changes can be difficult to unravel and correct, but if the spreadsheet in question happens to hold customer account details this could represent a PR disaster. Even worse, what if you a company were compiling its financial results and the data diddler altered these figures?

Another particular concern is the increasing use hackers are making of backdoor Trojan horses or Remote Access Trojans (RATs). This code allows hackers to gain remote control of a PC across the Internet even if they are located on the other side of the world. With a RAT, hackers can view what is on the infected user's machine, steal data, take control of the remote keyboard and mouse and even send emails using the infected computer's username.

Virus infection can also compromise a company's reputation. In 1999, Fuji Bank became infected with a word macro virus called WM97/Class-D. At the time the bank was embarking on a merger, and was sending vital and sensitive information via email to potential investors. Unfortunately the virus managed to intercept one of these communications. When the document was opened its recipients were told that they were 'big stupid jerks'. Not the best way to impress potential business associates...

The Fuji Bank example is an extreme case, but every financial runs the risk of damaging its reputation if it becomes infected with a virus. Today, many commonly encountered viruses are capable of scooping up confidential documents and spreadsheets from the infected computer, and distribute them across the Internet. Again, these may pose a serious risk to the fortunes of financial organisations.

Anti-virus software has a crucial part to play in protecting against computer viruses - but no vendor can provide a perfect solution. Some anti-virus companies are now releasing technology which reduces the threat by blocking suspicious filetypes, or files with double extensions, at the email gateway. This can dramatically reduce the chances of a network's security being breached by a new or unknown virus.

Vendors are also incorporating heuristics into their products, these search for and block 'virus-like' characteristics. Again, heuristics technology guards against future viruses, but it does run the risk of throwing up false positives (where the software false alarms on emails and code which are not strictly viral). Here the impact can be as great as a real virus infection; IT managers are just as likely to close down mail servers over a false alarm as they are with real malicious code.

To be effective, software must be updated on a frequent basis. In April 2002, 80 percent of calls to Sophos's helpdesk were from users infected with the relatively virulent Klez worm. Users were still becoming infected even though protection against this worm was issued some two months earlier. To counter this, some companies are now choosing to outsource these updates to the IT security solutions providers. However, in the financial sector particularly, some businesses are reticent to lose control of these vital network elements, opting instead to manage updates in-house.

There are other measures that can be introduced. Policies advising users not to open unsolicited attachments or download material from the internet help combat viruses and are completely free to implement. Some companies are also reducing the risk of infection by restricting users' web access - this helps protect against viruses such as Nimda which can be contracted simply by visiting an infected website.

Viruses are a serious threat to financial institutions but they do not herald the Cyber-Armageddon predicted by many IT security 'experts'. A comprehensive anti-virus strategy, combining products and policy, will ward off the vast majority of dangers and will underpin the relationships of trust so crucial to the financial community.

# British Government takes on MessageLabs to bolster virus protection

- Government adds new line of defence against new breed of viruses
- Departments throughout government are now protected in a deal worth over £1 million
- Email security ‘critical’ to Government

The British Government has taken on email security company MessageLabs to further protect itself against the threat of destructive mass mailing viruses, in a deal worth over £1 million.

Departments throughout the Government, including the Treasury, Prime Minister’s Office, Department of Trade and Industry and Ministry of Defence, will now be protected by a new line of defence against the growing dangers posed by mass mailing viruses such as Lovebug, Sircam and Goner. This move will ensure that any threats are identified and stopped before reaching the Government’s network boundaries.

While business continuity and Internet security are important for any organisation, for the UK Government they are imperative. Any network downtime caused by a mass mailing virus could be critical for the Government, which relies greatly on email communications and Internet related applications to carry out a multitude of responsibilities.

The GSI (Government Secure Intranet), which provides the secure network infrastructure for all Government departments, decided to take on additional anti-virus protection due to the recent growth in mass mailing virus outbreaks and the inability of traditional anti-virus software to provide sufficient protection against these threats.

MessageLabs, the British owned email security company, will supply the GSI with its renowned managed anti-virus service, scanning emails at the Internet level before passing them on their final destination. MessageLabs uses patented artificial intelligence to pro-actively identify new virus outbreaks without the need for signatures.

MessageLabs service has proved itself by instantly identifying and stopping all recent virus outbreaks including Lovebug, Sircam, Nimda and Goner. While the GSI was trialing the MessageLabs service in late 2001 it was put to the test when the Goner virus broke out. MessageLabs stopped the virus immediately but its records showed that 21,167 copies of the destructive virus had been directed at Government email users over the first three days of the

outbreak. Although none of the viruses got through, the scale and speed of the outbreak confirmed the need for a further layer of protection.

Cable & Wireless, a MessageLabs partner, provides the infrastructure for the GSI and the anti-virus service has been delivered through them.

Ben White, CEO and Joint Founder of MessageLabs, said:

"Attack from email viruses is a clear and present danger for the Government, and the consequences could be very serious indeed. For example, the Goner virus last year actually deleted security software and other executable files from networks while SirCam emailed private documents around the globe.

"We are delighted that our email security service will now protect the Government and ensure that any threats are stopped well before they reach their network boundaries. This will ensure that the Government can get on with the very important job of running the country and encouraging greater adoption of Internet technologies, without running the risk of any virus related disruption. Our 100% record in stopping viruses, both known and unknown, means we are the best people to do the job."

Bob Evans, Director of Information Assurance and Resilience at the Office of the e-Envoy said:

" Effective information assurance needs a robust, effective anti-virus service. The MessageLabs service will therefore be a vital asset in protecting government systems against external threats and ensure that we comply with Sir Richard Wilson's recent comment that "Information assurance is right in the centre of the playing field… It is important for government to have its own house in order".

The MessageLabs service portfolio is available in Hong Kong as YKScan from Yui Kee, and is a complete email security solution that also scans email for pornographic images and 'spam' thus protecting customers from all the major threats.

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