Yui Kee Computing Ltd.

Newsletter

July 2002

Contents

Incident Update

Despite the appearance of W32.Datom.Worm, rated as a Level 3 threat by Symantec, around the 24 July, W32/Klez.H remains the dominant virus. As previously mentioned, its' feature of forging the senders' address makes tracing the source impractical so users of infected machines are not informed about the problem.

Sophos and Yui Kee Prepare Anti-Virus Guidelines for Schools

Sophos, a UK-based world leader in anti-virus protection, has released a series of information packs in English outlining how schools can protect themselves against virus attack. Yui Kee Computing has translated the packs to Chinese for use in Hong Kong. The first set of guidelines, produced for use by teachers, includes advice on safe computing procedures, describes the different types of virus threat and offers suggestions for classroom activities. Sophos has also produced, and Yui Kee has translated, two sets of guidelines for pupils - one for primary and one for secondary students. All these resources are now available free of charge on the Hong Kong Education City website.

Sophos issued these guidelines as a resource to complement the UK National Curriculum. Although information and communications technology is now taught in every UK school, little provision has been made for the teaching of safe and ethical computing. Yui Kee has noted that the situation is similar in Hong Kong.

Sophos and Yui Kee hope these guidelines will inform teachers and pupils not only of how to defend against viruses, but also of the dangers of writing and distributing them.

eToken for Microsoft Network Logon

Aladdin has announced the official release of their eToken solutions for Microsoft Network Logon.

Windows domain controllers offer a variety of integrated network logon schemes, from simple username + password to full, PKI based Smartcard authentication. eToken now enables implementation of strong two-factor authentication when logging on to Windows NT, 2000 or XP Domains.

To log-on to the network, a user simply inserts the eToken into the USB port and enters the eToken password, which is set by the user.

Denial of Service

Nine years ago, Wolf Djupedal catalogued over 14,000 books and magazines written in New Norwegian and stored the catalogue in a password-protected dBase IV file. He died without revealing the password. Recently, Kirsti Langstoyl , librarian at the Ivar Aasen Centre for New Norwegian Culture in Oresta, Norway appealed for help in unlocking the database, and security specialists across the Internet have come to her aid.

Fortunately, dBase IV encryption is not very strong, and experts already seem to have succeeded in accessing the data. Data protected by strong encryption could easily be lost forever in similar circumstances, constituting a denial of service attack. Organisations should consider this issue carefully whenever data encryption is proposed. Firstly - is the encryption necessary? It is unclear in this case why the catalogue ever needed to be encrypted - it was intended to be a public resource. Secondly, how can the keys be managed to protect the data and still permit authorised access when staff leave suddenly or die.

More details at these sites:

http://www.idg.com.hk/cw/readstory.asp?aid=20020606005

http://www.silicon.com/ebcs53801

http://news.com.com/2100-1001-934060.html

First JPEG Virus?

A recently released virus, W32/Perrun-A has the capability of modifying JPEG (image) files to include part of the virus code. Vincent Gullotto of Network Associates has bee quoted as saying "Because JPEGs are a common image format on the Web, the virus poses a risk of infecting any user who views an infected file on a Web site. Users would have to have the executable on their systems for this to occur." This is a strange thing to say, the executable is part of the virus, so, in effect, "any user" who is already infected may be infected by viewing an image on a website. This is also obvious from the name assigned to it by Network Associates and other anti-virus developers: W32/Perrun-A, indicating it is a 32-bit Windows executable - the .exe file must be present for the virus to work.

For a more reasoned description of W32/Perrun-A, see:

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

To provide some practical advice for users, do not worry about viewing or downloading images. If your anti-virus software reports W32/Perrun-A on your system, follow the developer's removal instructions, and, to be certain there are no corrupted JPEG's left, scan all files. In fact, it is a good recommendation when cleaning up after any infection to scan everything as a check at the end.

Privacy

Privacy groups are very concerned about the European "Electronic Communications Data Directive", which gives states in the EU the right to look at emails in criminal cases, and in the interests of "national security". The directive also covers cookies and spam.

More information:

http://www.silicon.com/ebcs53700

Best Practice

Sophos has issued guidelines on "Best practice for multi-tier virus protection", summarising how viruses can be fought at different levels in an organisation.

http://www.sophos.com/virusinfo/whitepapers/multi_tier.html

EICAR Conference

This year, the European Institute of Computer Anti-Virus Research conference was held in Berlin at the Forum Hotel. This was the eleventh EICAR conference, and also the first time they held a Doctoral Consortium. This idea of Tugkan Tuglular was an innovation aimed at helping M.S. and Ph.D. students produce Anti-Virus or e-Commerce related theses, and to enter the job market. The seminars in the Consortium included the hot issues in computer security research, general advice on Ph.D.s, and the opportunity for the students to discuss their projects.

Interesting aspects of the EICAR conference are its' academic leaning, now strengthened by the Doctoral Consortium, and its' involvement with European Community initiatives, including the EC Convention on Cyber Crime.

Nimda from Microsoft

Microsoft shipped Visual Studio .Net development toolkit CDs that were infected with the Nimda virus to South Korea in mid-May. The incident occurred due to a Nimda outbreak and the failure of a quality assurance process at a South Korean company that Microsoft contracted to work on the CD contents. This a a practical demonstration of one of the hardest problems in security - making sure that business partners are following the same high security standards that you have in place.

More details are at http://www.idg.com.hk/cw/readstory.asp?aid=20020617005.

Apache Vulnerability

A serious vulnerability in the most popular web server software on the Internet, Apache, was announced on 17 June. CERT/CC and the Apache Software Foundation issued advisories describing the flaw:

http://www.cert.org/advisories/CA-2002-17.html

http://httpd.apache.org/info/security_bulletin_20020617.txt

In most situations, this can permit a Denial-of-Service attack, and, in some cases, arbitrary code can be run on the server. On 20 June, Apache Software Foundation released new versions (1.3.26 and 2.0.39) that fix the flaw, and a new security bulletin:

http://httpd.apache.org/info/security_bulletin_20020620.txt

The serious vulnerabilities that have been discovered for Apache are few and far between, but this incident demonstrates the Apache Software Foundation's ability to respond promptly. This should help reassure organisations that are worried about Open Source software support.

All users of Apache should download and install the latest versions.

Security is not an "Optional Extra"

Allan Dyer

Security is not an "optional extra", it's obvious, so why am I bothering to mention it? Because there are so many cases where security is left out for various reasons.

"Let's get it running first, then make it secure" This is the pioneering attitude that has produced a lot of the Internet as we know it. It is a great way of moving forwards when trying to develop TCP/IP on isolated networks, or inventing the World Wide Web in a European nuclear physics research institute, it doesn't matter when experimental systems are unreliable. However, production systems should be better. Too often, the move to a more secure version is delayed, and, as it is delayed, it becomes a more difficult and complex problem. We face a slow move towards IPSec and IPv6; and SSL is still not used everywhere it should be.

It is more difficult to understand why the same attitude is accepted for systems that were always intended to be production systems. Open email relays and web servers exhibiting old vulnerabilities fall into this category; the installer or administrator seems to assume that, because it works, their job is done. There would be a lot less high-profile webpage defacements or spam if lockdown was a standard part of installation.

Unfortunately, application developers may require operating systems to be configured less securely. For example, Windows 2000 has many restrictions on members of the Users group (intended for ordinary users), preventing them from changing registry settings or deleting important system files. However, many "legacy applications", including ones from Microsoft, require additional "Power User" rights, that give them (or the viruses they may, inadvertently, be running) more freedom to damage the system. You can lock down Windows 2000 very securely, but you will get a lot of user complaints.

"The users cannot do that, so it is not a problem" This attitude is usually a misstatement of a fact, 'the users have not been given a way to do this", and the difference between them leaves an opportunity for an innovative ab-user. This gives us flaws like web "Shopping Baskets" that allow a user that understands cookies and HTTP to modify the prices charged to their credit card. The webpage forms that allow malformed input to result in arbitrary requests to a back-end database can be counted in this category too - yes, the CGI application should have validated the input, and handled potentially dangerous characters, like '," or ; - but there should be defence in depth. Why should a CGI script have user rights in the database to do anything it likes, including list all credit card numbers? It does not need the rights, but often it will have them, because it is easy, and the script *does not give the users a way to do it*.

"Users education is a waste of time" This attitude points at the many mistakes that users make, and claims that, because users continue to make mistakes, they are incapable of learning and therefore cannot be trusted with any aspect of security. An alternative attitude that is functionally equivalent claims that we are responsible for security, and if we ask the users to learn something to protect themselves, we have failed - users should not be required to learn about security. User education, however, is an essential part of information security management. Without it, users will be very inventive at circumventing protective measures; they will be your worst enemy. Education can change them into your best ally.

Security, then, is not optional; it should be considered and built in from the earliest stages, unlikely attacks should be considered, and defence in depth implemented, and the users should understand their part in the security, and be taught to fulfil their responsibilities.

Yahoo! Corrupts

Yahoo! has recently taken to modifying its' users' emails in an attempt to protect against malicious scripts. Words that are commands in some programming languages get replaced by other words with a similar meaning, but no programming function. Thus, mocha is replaced by espresso, eval by review and expression by statement. I would have thought that anyone who uses the word mocha cares that it is different from espresso - other people would just say coffee. The change is also made if the blacklisted word is part of a longer word, so evaluate might become reviewuate.

A search for reviewuate on Google found 170 web pages, and, in the first thirty of those, two were links discussing Yahoo's actions. The rest were webpages discussing topics including stock markets, junior fiction, peace education, and Chinese language degree courses. Congratulations, Yahoo, you have created a new word!

Yahoo! spokesperson Mary Osako said, "To ensure the highest level of security for our users, Yahoo! employs automated software to protect our users from potential cross-scripting violations," Ms Osako is forgetting there are three aspects of security: Confidentiality, Integrity and Availability. By modifying emails without authorisation, Yahoo! is destroying their integrity. They are also making some people who sent their latest web page updates via Yahoo! look rather foolish.

So how can we protect against scripts in email, without mangling the writer's meaning? The simplest method is very effective: do not use an email client that executes scripts, i.e., use something other than Microsoft Outlook. I have met no one who claims they need such a flawed email client. An up-to-date anti-virus scanner will find most other nasties in email. When something is found, the email should be blocked, not modified, and appropriate people notified.

Searching for particular words can be useful, to block obscenities, for example, but it is a very crude method to employ for looking for executable code. It should also be applied with thought - I have heard one report of a major drug company blocking the word "sex". One might expect legitimate emails in a drug company would contain that word, for example, in discussions of clinical trials, or if they have products specific to one or other sex. Also, all their employees in the English county of Essex could not send or receive email until the block was lifted.

More information:

http://www.internetnews.com/dev-news/article.php/1429061

http://story.news.yahoo.com/news?tmpl=story&u=/nf/20020719/tc_nf/18665

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