Yui Kee Computing Ltd.

Newsletter

December 2002

Contents

Editors Notes

Seasons Greetings as we draw to the close of another year. Looking at my own in-box, there seem to be fewer greetings with executable attachments than last year, perhaps users are learning about the risks (or perhaps users who send me greetings just want to avoid my friendly warnings). More people are sending links to web-pages, this makes sense: it saves bandwidth if you have grown tired of animated snow and choose not the follow the link (you still got the essence of the message: holiday greeting plus senders name) and it is no more risky for the recipient than going to a web-site with a securely-configured browser.

Taking the risk of looking foolish in twelve months, I will make some predictions:

- The top virus for 2003 will still be Klez. It first appeared in October 2001, it has dominated 2002, and it shows no signs of going away. I expect it will top the monthly lists for at least seven months of the year, and still be in the top 5 next December.
- There will be a small number of viruses for PDA's or other mobile devices. They will not spread well, because the numbers and connectivity of such devices is still too restricted.
- There will be an accelerating number of security flaws found and hacking attempts on Linux and Open Source software. This is because the popularity of Linux and Open Source software will continue to grow as more realise its' advantages, thus making it a more prominent target. The Open Source Community will demonstrate its' ability to effectively deal with the security flaws.
- Email will continue to be the most common route of virus spread. I hesitate to call this a prediction, it seems so obvious, but it is really saying what will **not** happen: there will not be a new, wildly successful virus spreading method that overtakes email in 2003. The most common route of virus spread will change as the computing environment changes: mobile devices and .NET will increase in 2003, but won't become the mainstream.
- A major security flaw will be found in Wind… No, I'll stop before I predict that the sun will rise.

Have a safe and prosperous year.

Allan Dyer

Incident Update

W32/Klez.H@mm is still the most common virus, and no major new viruses were found. A new variant of CIH, W95/CIH.1106, was discovered, as this is the first in four years it is curious, but it is unlikely to spread much as it only works under Windows 95 and 98.

SSH Vulnerabilities

CERT/CC has issued an advisory (CA-2002-36) that Secure shell (SSH) protocol implementations in SSH clients and servers from multiple vendors are susceptible to various vulnerabilities, including buffer overflows.

The CERT advisory confirms that the SSH products Yui Kee sells, from SSH Communications Security and F-Secure, cannot be exploited using the vulnerabilities.

Rapid7 found the vulnerabilities by developing a suite (called SSHredder) to test the SSH transport layer. Further details:

http://www.kb.cert.org/vuls/id/389665

Sophos Defends Financial Giant From Virus Attack

Sophos has been chosen to defend Aviva (formerly CGNU), one of the world's largest financial services groups, against virus attack.

Sophos Anti-Virus has been selected to protect 35,000 desktop computers in a deal covering the next five years.

Further information: http://www.sophos.com/link/aviva

Information Security Summit

Planning for an Information Security Summit, to be held in Hong Kong in November 2003, has started, a Call for Expressions of Interest from the organising committee is attached at the end of this newsletter.

F-Secure Data Security Summary of 2002

F-Secure characterises the data security world in 2002 by new types of threats. Virus outbreaks in Linux systems, attacks utilizing open source code, breaks into home computers and increasing activity of Asian virus writers kept data security companies busy. Known viruses today amount to some 80,000.

However, they noted that the number of serious outbreaks was lower than 2001 and no mobile or PDA viruses were seen. They cited a more strict attitude towards crimes directed at the society in the USA since September 2001 for the considerably decrease in the number of viruses from the US.

"Attacks against data systems will increase and they will become more and more professional. New, fast network worm technologies may lead into a situation where a worm spreads around the world in just a few minutes after it has been launched. These attacks can be done by hackers, hactivists, industrial spies, terrorist groups or organized crime. Society must be able to function in spite of such network warfare," says Mikko Hypponen, Manager of Anti-Virus Research at F-Secure.

Further information: http://www.f-secure.com/2002

Good Advice?

Allan Dyer

A Hong Kong ISP has sent its' customers advice on guarding their networks during the festive season. It would be nice to see ISPs helping their customers with their security more - if they gave better advice. Here are their DOs and DON'Ts, with my comments:

- DON'T open or forward anonymous emails

  This rule might help you avoid a little spam. While anonymous emails are strange, they are not a particular security risk. Most email-aware viruses will use the victim's address or forge the address, so you will probably receive viruses in emails from an address that you might recognise and trust. Treat **any** unexpected email with suspicion.

- DON'T open emails of strange file name

  Unfortunately, we are not told what a strange file name is. Don't open **any** attachments that you were not expecting. A double file extension, like iamavirus.txt.vbs is extremely suspicious, and should never be opened.

- DON'T open emails without a subject

  Like the first rule, it might help you avoid a little spam, but viruses usually make the subject attractive in some way.

- DO pay particular attention to emails received on 24 Dec, 31 Dec, 1 Jan, 14 Feb, Black Fridays as these are the beloved dates of the hackers

  Oh, and add the dates of festivals for other major religions, each country's National Day (hackers and virus writers are not restricted to particular religions or countries), dates of major events (June 4th, September 11th). Then add the virus writers' birthday, or his girlfriends', or the birthday of a famous person. For the record, I do not recall a significant information security event on Friday 13th in the past decade, but I have had quite a few press interviews on or just before the date in that time.

  The truth is that you need to be vigilant **every** day. There is a suggestion that more viruses are released near the end of the summer (are bored teenagers writing viruses in the long vacation, and releasing them before returning to school?), and others try to blend in with the rush of holiday greetings (remember W32/Ska.A, better known as Happy99?). There are viruses that trigger a payload on a particular date, but it is too late if you start checking your machine for CIH on 26th April! Also remember that Happy99 continued to spread well for two years, despite the obvious datedness of the subject.

- DO update anti-virus applications from time to time

  Yes, good, except, lets make that "as often as your anti-virus developer provides updates" - in many cases, this now means daily, or more frequently.

OK, ISP, nice to see you making an effort. Try harder next year.

Sophos Anti-Virus Beats All Competition In Comparative Test

In a comparative review of corporate anti-virus solutions Sophos Anti-Virus has been found to out-perform all competitors.

The tests, conducted by PC Pro magazine, praised Sophos Anti-Virus for its suitability for protecting businesses and showed Sophos clearly outclassing products from the likes of Network Associates, Symantec and Trend Micro. Sophos was awarded the top prize of "PC Pro Labs Winner".

Further information: http://www.sophos.com/link/pcpro

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/

FIRST ANNOUNCEMENT
CALL FOR EXPRESSION OF INTEREST - SPEAKERS & SPONSORS

INTRODUCTION

The Information Security Summit Organising Committee is issuing its first Call for expressions of interest to assist in the development of the Information Security Summit programme.

The Information Security Summit will be held over a **period of 2 days in November 2003** (exact date not yet determined) in a major **Hong Kong** hotel or in the Hong Kong Conference and Exhibition Centre.

The Summit will consist of **three concurrent streams** running over the course of the Summit. The primary **audience** of the Summit is expected to be middle to senior management and security professionals.

The primary communication language for the conference will be in English, however, where a proposal is submitted to present in Chinese, the Organising Committee will consider such a proposal.

If you or someone you know would be interested in presenting one or more topics, or in sponsoring the Summit, please complete the attached session proposal form and return it no later than **27th January 2003**. Send attached completed session proposal forms via e-mail only to **summit@bs-7799.com**.

SPONSORSHIP

Any company interested in being approached at a future date for **sponsorship opportunities** for the Information Security Summit should indicate this interest in the attached template. The organising committee will provide more detailed information of the conference format and logistics when following up interested organisations in the future.

SPEAKERS

This Call represents an opportunity for you to assist the organising committee in developing topics and being considered for allocation of a **speaking position** in the final programme.

The Organising Committee has identified some suggested topics for the Summit and has created a broad Summit framework. Respondents should not feel that they are restricted to this list of suggested topics and the Organising Committee is very interested in reviewing creative topics that may not have previously been considered for other security speaking events.

The **selection process** for speakers will place greater emphasis on proposals generally directed at middle to senior level management audience. Some technical level presentations will be included in the programme and interested parties are invited to submit such proposals. However a greater emphasis is being placed on the management level in terms of weighting applied to the final programme.

Proposals offering contributions in any aspect of information security are solicited for submission to the Information Security Summit Organising Committee. The theme for the event is “Capitalise the value of information security for competitive advantage”. Proposals may present management or technical theory, applications or practical experiences (e.g. case studies) on any form of information security topic including, but not limited to:

- Security Policy
- Access Control
- Anti-Virus
- Awareness
- Business Continuity Management
- Communications & Operations Management
- Information Asset Classification & Control
- Security Compliance and Governance
- Information Security Standards
- Information Systems Management Security Certification
- Personnel Security
- Physical and Environment Security
- Security Architecture and Models
- Security in Systems Development
- Security Incident Management

It is important to note that the focus of the Summit is on advanced and emerging information security topics, including advanced research, future development trends in information security, experience sharing and industry case studies. The Summit organising committee will evaluate speaker’s proposals on this basis. Additionally a very strong weighting will be placed towards accepting proposals that meet a criteria of providing an advanced focus on information security topics.

FIRST ANNOUNCEMENT
CALL FOR EXPRESSION OF INTEREST - SPEAKERS & SPONSORS

SUPPORTING PROFESSIONAL ASSOCIATIONS AND BODIES

The organising committee is represented and supported by the following associations and bodies:

- British Standards Institute (BSI)
- Hong Kong Computer Emergency Response Team (HKCERT)
- Hong Kong Computer Society (HKCS)
- Hong Kong Productivity Council (HKPC)
- Information Security and Forensics Society (ISFS)
- Information Systems Audit and Control Association (ISACA)
- Professional Information Security Association (PISA)

INSTRUCTIONS FOR PROPSAL SUBMISSION

Submitted proposals must be written in English and submitted through the use of the attached template.

Accepted proposals will be invited to submit a paper that does not substantially overlap with papers that have been previously presented or published in a journal or at another conference. A separate and more formal notice calling for submissions will be provided in March 2003 providing instructions for the submission of Summit presentations to successful proposers.

To submit a proposal, send an email to **summit@bs-7799.com** containing the title of the proposal, the authors' names, e-mail & postal addresses, phone & fax numbers & identification of the contact author.

INITIAL PROPOSALS ARE SOUGHT BY 27th JANUARY 2003.

PROGRAMME COMMITTEE CHAIR
DALE JOHNSTONE

PROGRAMME COMMITTEE

Andy Ho	SC Leung
Frank Yam	Vincent Chan
Jimmy Pang	Vincent CC Chan
Patrick Li	Vincent Yeung

KEY DATES

Submission of Initial Proposals: 27th January 2003

Notification to responders: March 2003

Further information can be obtained be sending an electronic mail message to the Organising Committee at **summit@bs-7799.com**

INFORMATION SECURITY SUMMIT – HONG KONG (NOVEMBER) 2003

CAPITALISE THE VALUE OF INFORMATION SECURITY FOR COMPETITIVE ADVANTAGE

FIRST ANNOUNCEMENT

CALL FOR EXPRESSION OF INTEREST - SPEAKERS & SPONSORS

PLEASE COMPLETE THIS TEMPLATE TO EXPRESS YOUR INTEREST

My company is interested in being approached to sponsor this event **YES** **NO**

I am interested in being considered as an event speaker **YES** **NO**

Company Name _____

Contact Name _____ Please also attach a list of prior speaking and educational engagements, biographical sketch (c.v., resume, work experience, et cetera)

Contact Title _____ e.g. Chief Security Officer, Security Manager, Audit Director

Contact Address _____

Telephone _____ Facsimile _____

E-Mail _____

TOPIC PROPOSAL

Topic Area _____

Suggested Title _____

Brief Topic Outline _____

Target Audience _____ e.g. Beginner, Intermediate, or Advanced, attendee knowledge level, experiences, et cetera

Audience Benefits _____

Presentation Format _____ e.g. Lecture, Demonstration, Panel, or "Hands-on" Workshop

Length Of Session _____ Currently sessions have established for a period of 45 minutes. Alternative proposals will be considered.

Abstract

(narrative description) _____

Please submit your proposal to ***summit@bs-7799.com***


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