
**Yui Kee Computing Ltd.**

# Newsletter

September 2002

## Contents



## Incident Update - W32/Bugbear.A

W32/Bugbear.A, also known as I-Worm.Tanatos or W32/Tanat, is an internet worm that spreads via email. Current information is preliminary, but, when executed it will install itself to run each time the machine is started, and it also terminates various anti-virus and firewall programs, and contains a keystroke-logging program. It sends itself to email addresses found on the victim's machine. The message subject and body are quite variable, and may be related to text from other files or messages on the machine. W32/Bugbear.A also opens a backdoor, and is capable of spreading via a local network by copying itself to the startup folder on remote shares.

Most anti-virus developers have issued alerts about W32/Bugbear.A. Messagelabs first stopped it at 20:23 GMT 29 September 2002 in an email from Malaysia. Sophos has received several reports in a short space of time.

Users are advised to update their anti-virus software as soon as possible.

## AVAR 2002 Conference Preview

As we head towards the close of the year, the highlight of the anti-virus calendar in Asia approaches. Now in its' fifth year, the Association of Anti-Virus Asia Researchers International Conference will be held in Seoul, Korea on 21 - 22 November. Previous years have seen the event grow to about 180 participants from around the globe.

Following the trend of previous years, several speeches are reports from government agencies in the region. Seung-Cheol Goh of the Korea Information Security Agency will cover the incident response of the Korean Government, with particular reference to the efforts made for the 2002 Korea and Japan World Cup. Zhang Jian of the China National Computer Virus Emergency Response Center will survey the situation in China, including dealing with a new virus found in China and testing of anti-virus products. Shigeru Ishii of the Information technology Promotion Agency in Japan will summarise the results of their computer virus infection surveys in Japan and overseas. The surveys also show usage rates of anti-virus software on clients, servers, groupware and gateways, and rate of pattern file update, which should interest developers, to see how their software is really being used.

As a counterpoint to these government reports, Costin Raiu will present an outsiders' view of anti-virus protection in Asia. What can a Romanian say about Asia? Quite a lot, by using statistics from his "Smallpot" project - a very specific honeypot used to monitor CodeRed, Nimda and Spida infections, Mr Raiu will provide a review of the average security status of the large mass of computers connected to the Internet in Asia.

Larry Bridwell will add data from America to the debate and show how the problem is out of control. I certainly look forwards to seeing what new insights can be gleaned by comparing and contrasting the data from these disparate sources.

Policy is the foundation that information security is built on, and Takuya Yamazaki of the Ministry of Economy, Trade, and Industry Deputy in Japan will present the most current concept and views of information security policy of Japan, indicating the boundary of the role between public sector and private sector.

The management level is also addressed. In the second day keynote speech, Jimmy Kuo will review the year. Always and entertaining speaker, Paul Ducklin will tell us how to avoid being a victim. Looking at blended threats, Motoaki Yamamura will provide a big picture view of what computer systems managers need to know now in order to stay ahead of emerging viruses and hacking techniques.

Some presentations are definitely heading towards the technical aspects. Alex Shipp will discuss the different strategies useful for desktop and Internet level anti-virus protection. Randy Abrams will describe and demonstrate the automated virus scanning system in use at Microsoft. Jong Purisima addresses the increasing problem of malware that targets systems as a whole and the future of System Disinfection.

Naming, apart from providing a rare opportunity to quote Shakespeare in an anti-virus context, has been a controversial topic for a long time. Nick FitzGerald will take the rose by the thorns and make the first public presentation of the Revised CARO Naming Convention.

Then there are the firmly technical speeches. Vesselin Bontchev and Katrin Tocheva give the keynote speech on the first day, discussing the future of macro and script polymorphism. Last year, Dr. Bontchev's keynote on the responsibilities of the anti-virus researcher prompted some debate so I am sure this will be an eye-opener.

Won-Hyok Choi will discuss how to detect and repair viruses that hook the Windows API and attack Win32. Turning this around, Yoshihiro Yasuda will consider the appropriate Win32 hooking that can be used for malware analysis and the design of research tools.

SiHaeng Cho will discuss the influence of double-byte character sets in script viruses and worms, and how to prevent this from influencing the integrity of anti-virus software. Completing the line-up, Myles Jordan will discuss metamorphism, its evolution and the application of a meta-heuristic system to detect this latest generation of viral techniques.

The programme also features a panel discussion, banquet, the AVAR AGM and a hospitality programme. Overall, the programme covers the full range, from Government policy down to the last technical bit. To close with the words of the Conference Chairman, Charles Ahn, "The dream of building a robust information society can become a reality only when information security is guaranteed, and I believe, the 5th AVAR International Conference will be the small yet meaningful step toward that dream."

**Conference:** AVAR 2002
**Dates:** 21-22 November 2002
**Venue:** Ritz-Carlton Hotel, Seoul
**Web:** http://www.aavar.org/avar2002/index.html

# Sophos Anti-Virus receives West Coast Checkmark for 100% detection of in-the-wild viruses yet again

Sophos announced at the beginning of September that its flagship product, Sophos Anti-Virus, has yet again achieved West Coast Labs Checkmark certification.

Sophos Anti-Virus version 3.60 for Windows 95/98, Sophos Anti-Virus version 3.60 for Windows NT Server and Sophos Anti-Virus version 3.60 for Novell NetWare have again successfully been awarded Anti-Virus Checkmark level 1, providing further independent verification that Sophos is capable of protecting against all known 'in-the-wild' viruses in both on-demand and on-access modes.

West Coast Labs, an independent research and test centre, have developed the Checkmark system. It provides a reliable means of authenticating those products that users can consistently rely upon to provide the highest quality anti-virus solutions.

"Sophos Anti-Virus has an enviable record in comparative tests by independent laboratories," said Graham Cluley, senior technology consultant at Sophos. "This is the latest in a long line of accolades already received this year - we're delighted to have had the quality of our software verified by the experts at West Coast Labs."

More information about positive test results and certifications received by Sophos Anti-Virus can be found online at http://www.sophos.com/products/reviews/

# F-Secure Plays Key Role In Slapping Down Slapper Worm

The threat of the Linux Slapper worm has been nullified by proactive anti-virus work by specialists at F-Secure. In what is believed to be the first action of its kind by an anti-virus company, F-Secure was able to identify exactly which Web servers were being infected as each infection happened, send a warning to the administrators of the infected systems, and offer a free version of F-Secure Anti-Virus for LinuxTM to remove the worm from their systems.

Across the weekend of Friday 13th, following the discovery of the worm, F-Secure anti-virus laboratory was able to reverse-engineer the peer-to-peer protocol that the worm exploits to infect machines. This enabled F-Secure to access to the Slapper attack network by posing as an infected web server. Through this false server, F-Secure was able to determine the exact number of infected machines and their IP addresses as each server became infected.

In the process of warning the administrators of the infected servers, F-Secure worked in concert with 14 national CERT organizations. This approach was highly appreciated by many companies with emails: "Thanks kindly for your warning; our customer tells us they have upgraded their server. Congratulations on a job well done." Hugh Brown, Dowco Internet.

According to Mikko Hypponen, F-Secure's Manager of AV research: "Slapper was a very real risk, because its peer-to-peer networking capability enabled the author to take over any or all of the infected servers. The risk was not just distributed denial-of-service attacks, but also the backdoor access and control capability it gave over key parts of Internet infrastructure. That's why we took these measures to counter the risks it presented."

According to F-Secure, Slapper is representative of a new breed of worms and viruses as it is as much an attack tool as it is a quickly spreading worm.

F-Secure's Global Slapper Information Centre provides regularly updated information on the worm and numbers of infected servers categorized by the top-level domain. The company says it is imperative that all servers are cleaned and patched to prevent future infections as soon as

possible - both to stop the spreading of the worm and to prevent unauthorised access to the infected servers.

Global Slapper Information Centre can be found from:

http://www.f-secure.com/slapper/

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