Yui Kee Computing Ltd.

Newsletter

July 2003

Contents

Incident Update

There have been no major incidents, and W32/Klez.H@mm is still the most common virus in MessageLabs statistics. However, there are some continuing trends:

W32/Warpigs.B takes password guessing to new lengths - it contains a list of 1600 passwords that it uses when scanning the network for vulnerable hosts.

The W32/Webber Trojan arrives in an email that uses people's sensitivity about their personal data to encourage the recipient to open the attachment. The email message appears to be a failed loan or credit card application from a well-known institution, and claims that the attachment is the recipient's credit profile. Of course, opening the attachment launches the Trojan.

Warpigs and Webber are not common, but there are other similar ones so reminding your users about Safe Hex might be a good idea.

Vulnerability Update

The U.S. National Infrastructure Protection Center (NIPC) has updated their advisory concerning the RPC vulnerability in Microsoft operating systems. They note that there has been increased scanning for the vulnerability on the Internet recently, so they recommend patching affected systems or blocking TCP and UDP ports 135, 139 and 445 at the perimeter.

Savvy System Administrators will have done one, or probably both, of these already, so this is a reminder to the technical staff: don't just remind users about Safe Hex; practice it yourself.

More information:

http://www.nipc.gov/warnings/advisories/2003/Potential7302003.htm

http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp

http://www.theregister.com/content/55/31957.html

Virus Writer Looses Appeal

The Welsh virus writer that created the Redesi and Gokar worms, Simon Vallor, lost his case at London's Court of Appeal on 21 July. The worms are thought to have infected about 27,000 computers in 42 countries. Vallor was convicted and sentenced to two years jail at Southwark Crown Court in January.

His lawyer argued that the sentence should be reduced because Vallor's relative youth (he is 22), previous good character and that he did not realise how much damage his viruses would cause. The judge, Mr. Justice Aikens, dismissed the appeal, saying that the crimes were "calculated and disruptive". On hearing of the failed appeal Allan Dyer, our Chief Consultant, commented, "Almost every virus writer who has been caught has used the same excuse, that they misjudged how much it would spread or how much damage it would cause, I am glad to see that the Judge was unimpressed by it."

This is only the second conviction in the UK for writing and spreading a virus and the sentence is thought to be the harshest imposed on a virus writer anywhere. A UK court sentenced Christopher Pile to 18 months in 1995 for spreading several viruses. Other convicted virus writers include David Smith, the author of the Melissa virus, who was sentenced in the USA to 20 months and Jan de Wit, author of the "Anna Kournikova" worm, who got away with 150 hours community service in the Netherlands. However, under UK law, Vallor could have been sentenced to up to five years. Allan Dyer was pleased with the sentence, "It was not excessive, both in terms of the maximum permitted sentence, or compared to the time it would take one person to disinfect 27,000 computers, and it is enough to send a clear message to potential virus writers. Let's hope they are listening."

Most virus writers are never identified, but Vallor is reported to have been tracked down by the FBI and North Wales police after he boasted of his achievements in an internet chatroom.

Sophos Anti-Virus enters Mainland China market

Certification from Ministry of Public Security enables Sophos to deliver anti-virus protection to businesses on the mainland.

Sophos, a world leader in anti-virus protection for businesses, has announced that its award-winning anti-virus software has been certified for use in Mainland China. Issued by the Chinese Ministry of Public Security, the certification enables Sophos to market and distribute its anti-virus solutions for Microsoft Windows platforms.

"The expansion into Mainland China is a key step in our aggressive campaign to increase our market share worldwide," said Dr Jan Hruska, joint founder and CEO of Sophos Anti-Virus. "The potential demand for anti-virus protection in China is overwhelming. Participation in this strategic market will help us grow our business well in excess of the natural growth of the anti-virus market."

According to a survey conducted by the Chinese Ministry of Public Security in October 2002, 84 percent of respondents stated that their computers had suffered a virus attack, up from 74 percent in 2001. The survey also revealed that 64 percent of respondents had lost data as a result of a virus. The survey, carried out by the Ministry's National Computer Virus Emergency Response Centre, had analysed the data of more than 6,000 respondents.

"Sophos can now assist these companies in protecting their systems against computer viruses," said Charles Cousins, managing director of Sophos Anti-Virus Asia.

Reports from IDC, a world-leading provider of industry analysis, state the Chinese software market is worth $6 billion (US), of which security software accounts for 34 percent. IDC added that several factors drive this market, such as greater awareness of security needs, upcoming e-government projects and increased demand of mid-range business market.

DNA Chips for Improved Security?

Allan Dyer

As my first degree was in Microbiology, I was intrigued when I recently noticed news about DNA chips being used for security solutions. A Taiwanese company called Biowell Technology has developed the technology, and is now marketing it through European and American partners for applications including anti-counterfeiting and access control, but is it really a breakthrough in security?

If I wanted to ridicule the company, their website (http://www.biowell.com.tw/) provides numerous examples of marketing hyperbolae and pseudo-science. They have, "applied the uniqueness of DNA into multiple media for anticounterfeit purpose" - but a primary characteristic of DNA is that it can be reliably copied, your body contains billions of copies of your DNA, identical twins demonstrate it may also be duplicated across organisms, and Dolly the sheep holds out the potential for any individual's DNA to be artificially duplicated. Apparently they aim to be the "leader in living biotechnology" - is there such a field as dead biotechnology?

But do their claims stand up to technical scrutiny? Biowell has two main types of security product: DNA-tagged inks and paints (further incorporated into labels) for anti-counterfeiting, and the DNA Chip, DNA bonded to an electronic circuit in an unspecified way, for authentication. They can also test parentage, but that is not normally considered a security problem.

Information is information, no matter how it is stored. The DNA in Biowell's inks, labels and chips is essentially storing information as a long base-4 number (mathematicians and biochemists might appreciate the double meaning of "base" here). How is the information used?

In the anti-counterfeiting products, it is treated as a unique secret identifier. Items with the correct identifier are genuine; others are fake. It is claimed that the DNA cannot be duplicated from the label, but statements that the label can be analysed and the DNA sequence compared with their database contradict this. If you can sequence the DNA from the label, you can feed the sequence to a DNA synthesiser, and produce unlimited copies of it. For field tests, they provide an easy-to-use one-time swab that will cause a genuine label to change colour. This only demonstrates that it is a label with the correct chemical composition, not that it has the correct sequence on its DNA.

When the DNA-chip is inserted into Biowell's reader, the interaction with the DNA generates a "unique analog signal" that can then be amplified, filtered, digitised and compared with a database. The "unique analog signal" is thus being used as a shared secret for the authentication process. It appears infeasible to recover the DNA from the chip for replication, but it is not necessary to duplicate the chip, it is only necessary to duplicate the signal it produces. This is a simple "replay attack". There is also the question of how many possible distinguishable signals there are. Although the DNA sequence length is reported to be "several million bases" the electronic interactions that produce the signal are unlikely to reflect the full subtlety of the sequence, especially after the filtering and digitisation.

The other strength of the products is that only Biowell knows how to make them so the source is controlled, but the traditional technologies of reverse engineering and industrial espionage can neutralise this strength. Security through obscurity is not long-term protection.

Biotechnology is currently "in vogue" but we should maintain a critical attitude in evaluating security products. Added DNA does not magically make a product more secure.

Copyright Myths

A former head of the U.S. Justice Department's computer crime unit explains the truth behind some myths about U.S. Copyright law in The Register:

http://www.theregister.com/content/6/32004.html

What is the Value of a Security "Seal"?

The names of the companies involved are omitted to focus attention on the flaws in the process. A local ISP has a nice little logo on their webpage, emblazoned with the phrase, "[Name One] Secure Site by [Name Two] Click to verify", where Name Two is a well-known international commercial Certification Authority, and Name One is a Recognised Certification Authority in Hong Kong. Clicking the logo opens a popup window titled "Certificate Information".

It is good to see companies taking security seriously, if they are doing it properly. Unfortunately, the ISP has placed the logo on an unencrypted webpage, and it is misleading to describe the link to the "Certificate Information" page as verification - the link can be used independently of the page or site the certificate information describes.

The certificate information page, served from an SSL server at Name One's domain, does give the full hostname for the server described, and a serial number and issuer digest - but it does not describe how these can be used to verify the "secure site" is the real one. It also says that all information sent to the "secure site", if in an SSL session, is encrypted, but does not mention how to recognise an SSL session.

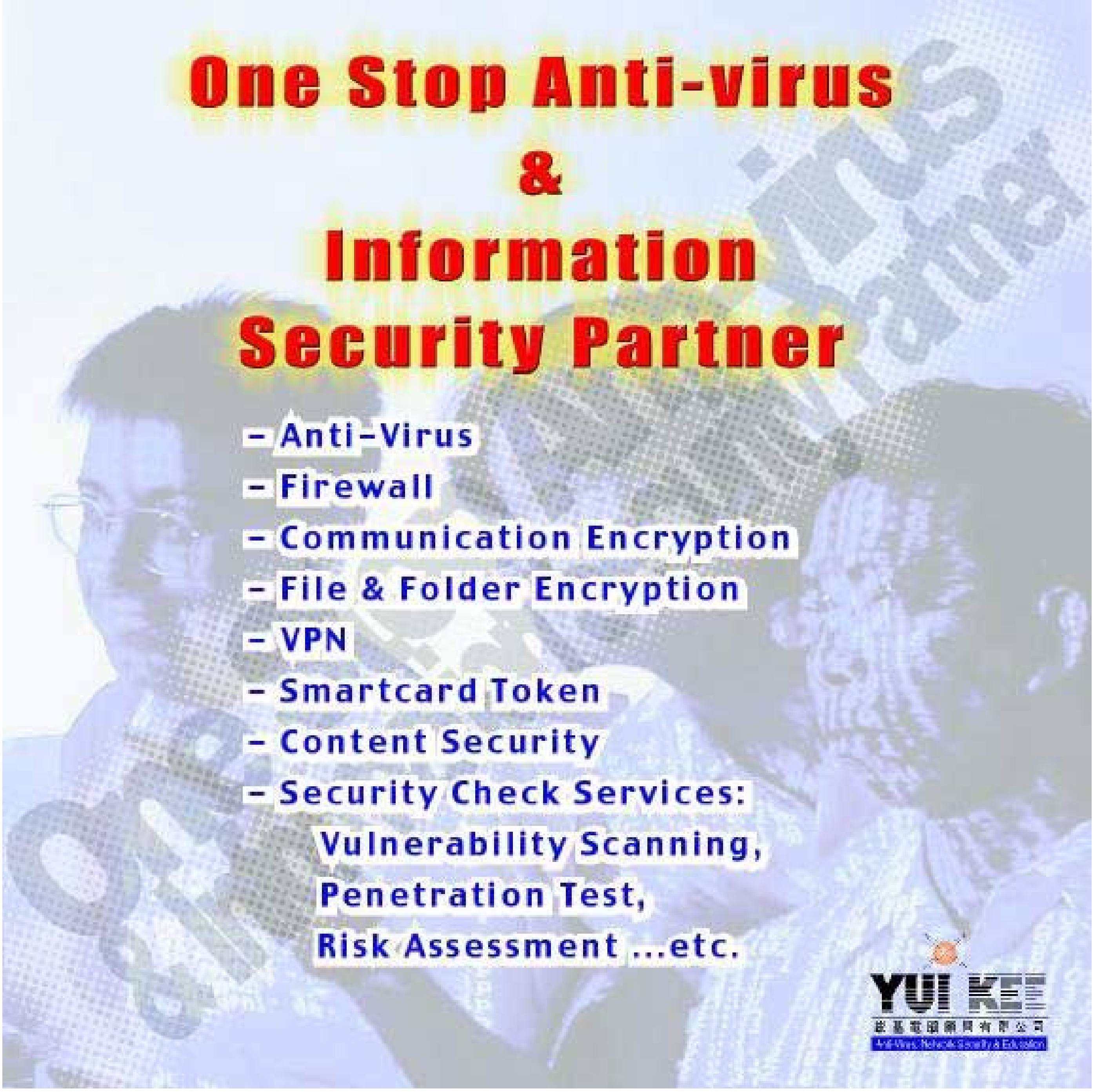
So, as the ISP has linked from an unencrypted page, most of the information is irrelevant. As the "Certificate Information" does not describe the steps necessary for verification, only someone who already knows how to check server certificates can use the information presented. All that is left is the assurance that, "[Name One] has verified the organizational name and that organization has the proof of right to use it." - it does not even give a Business Registration Number to help identify the organisation.

Can this logo do anything other than generate a false sense of security? We asked Name One for their feedback. They responded, "[Name One] is a company to provide quality products and services to our customers. We appreciate your comments and we will review the content of our website and make appropriate amendments if necessary."

Users already have a hard time understanding the intricacies of security; we hope this scheme can be amended to something more useful and less misleading.

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
銳基電腦網絡有限公司
Anti-Virus, Network Security & Education