Yui Kee Computing Ltd.

Newsletter

December 2003

Contents

Incident Update

There have been no major outbreaks. MessageLabs top five list is currently W32/Dumaru.A-mm, Swen.A-mm, W32/Mimail.J-mm, W32/Klez.H-mm and W32/Sobig.F-mm.

Microsoft Delivers Patch in "Patch Free Month"

On Tuesday, 9th December, Microsoft announced that they did not need to release any security patches this month. However, due to a bug in the Windows Update system, the patch for MS03-051, released on 11th November, was not delivered to some XP users last month. Instead, it was also delivered on 9th December, making the "patch free month" announcement confusing. Are these trustworthy computers?

Privacy Commissioner tells Mobile Operator to Improve Website Security

In a recent investigation (Case No. 200214122), Hong Kong's Privacy Commissioner for Personal Data found that a local Mobile Operator had contravened the requirement of Data Protection Principle 4 (Security of Personal Data) of the Personal Data (Privacy) Ordinance. An enforcement order was not issued because the company had already taken remedial measures to improve the security of personal data.

This is believed to be the first case where a Mobile Operator has been required to improve website security by the Privacy Commissioner. Data Protection Principle 4 states, "All practicable steps shall be taken to ensure that personal data … held by a data user are protected against unauthorized or accidental access…". The details of the case show that flawed security and procedures will not be considered adequate to fulfil this requirement and it is to be hoped that other Service Providers will take note and ensure they have appropriate security in place.

The investigation began in September 2002, when a complaint was made that the security of the Mobile Operator's website, where customers could view their bills, was inadequate. The billing website was protected by a username, password system, where the username was the customer's mobile number, and the password was 6 digits, with the default being the digits of the customer's ID card number. The system did not lock-out the account after repeated failed

login attempts. Thus, an attacker only knowing a person's phone number could guess passwords until they succeeded - a test demonstrated that a simple Perl script was able to find the password of a customer in less than a week, without causing any kind of security alert at the company. An attacker could then access personal information of the victim, including their full name, address, and phone bill details - in many cases, they would also have discovered the 6 digits of the victim's ID card number.

In November 2002, the Mobile Operator modified the website to fix these, and some other, flaws, but, in doing so, made the security of the site worse. The major new flaw that was introduced was in the password reset procedures. The website would lock an account out after 5 invalid login attempts. Users could then call the Mobile Operator's Hotline, and the password would be reset to a fixed number: "123456". This makes it trivial for an attacker to force a lockout, and set a process to periodically try "123456" until the victim calls the Hotline, and the password is reset, allowing the attacker access.

In October 2003, after the flaws in the procedures were pointed out, the Mobile Operator made further changes. When a customer calls the Hotline for a password reset, it is reset to a randomly generated 6-digit number and the password is sent to the customer's mobile in a short message.

The latest changes make unauthorised access far more difficult - while SMS messages are not guaranteed to be secret, an attacker would find it difficult to intercept the required message (unless the phone was stolen, when there would be a far more pressing reason to freeze the account).

It would be hoped that similar investigations could be completed in a shorter timescale in future.

Time of India Reporter Caught by Old Virus Hoax

On 17 December, the Times of India published a story headlined: "Microsoft Warning: Virus Alert!" (http://timesofindia.indiatimes.com/articleshow.cms?msid=358852); which details the "deadliest virus ever" that travels in emails with the subject "A Virtual Card For You". Experienced support personnel will instantly recognise this as a well-known hoax that first appeared around January 2001, described on most anti-virus websites, e.g.:

- http://www.sophos.com/virusinfo/hoaxes/virtualcard.html
- http://www.umich.edu/~virus-busters/hoaxes/virtual.html
- http://vil.nai.com/vil/content/v_98893.htm
- http://www.f-secure.com/hoaxes/vcredit.shtml
- http://www.virusbtn.com/resources/hoaxes/index.xml

The reporter concerned, Sharvari Joshi, demonstrates a lack of concern for journalistic standards by "quoting" both Microsoft and McAfee from the hoax, without checking with the actual companies concerned.

In the same article, the statement "It's a proven fact that 60 per cent of all these virus outbreaks are caused by someone in the anti-virus company, so that their latest vaccines can sell. That's why I believe that there's no reason to panic, since the companies will definitely come out with a counter-solution." is attributed to Deepak Shikarpur, computer expert and chairperson of Computer Society of India.

If this is the viewpoint of the Computer Society of India, then the Society is showing deplorable ignorance of the ethical standards that anti-virus companies adhere to and require of their employees. They should immediately publish their proof. However, perhaps it is more likely that this outrageous statement is another example of Sharvari Joshi's "professionalism".

Linux Kernel do_brk() Vulnerability

A vulnerability in the Linux kernel allows a malicious local user to escalate their privileges, kernel version 2.4.23 fixes the problem. Secunia announced the problem on 2nd December, and major Linux distributors, including Debian, Red Hat and Slackware, released an update the same day. The CVE name for the problem is CAN-2003-0961.

The problem is not rated as critical, but administrators should update their installations when convenient.

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