Yui Kee Computing Ltd.

Newsletter

September 2006

Contents

Editor's Notes

Panic! Confusion! The World is ending! Three zero-day vulnerabilities affecting Microsoft products have been discovered this month. CERTs are issuing advice like:

> "Don't open untrusted Office documents"
>
> "Don't visit untrusted web sites"
>
> "Disable Active Scripting"

When you consider the nature of trust, you might as well advise people to stop using the Internet and throw away their computers.

And yet, life goes on normally, and Symantec has decided that the risk posed by the Trojans exploiting two of these vulnerabilities is "Very Low".

How can both these views be valid? Unfortunately, until patches are available, each of these vulnerabilities offers attackers a way into our machines that we can only try to avoid, not block. CERTs need to offer advice for each vulnerability; and the best advice is to try to avoid the attackers. On the other hand, Symantec is offering a risk level for infection by a particular trojan. As trojans do not spread, your computer is only likely to be infected if an attacker targets you. The risk of a random computer being infected is miniscule, but the consequences could be catastrophic.

Ultimately, we have to accept that we live with our computers in a dangerous world and we need to continually judge the risks of our actions. The problems can only be solved at the source; in the short–term, for these three vulnerabilities, that means patches from Microsoft; but in the longer term we need to question the development process that builds massively complex software systems with unknown numbers of vulnerabilities. We can be certain that these are not the last zero-day vulnerabilities to be found; some bad guys probably know about and are exploiting vulnerabilities we know nothing about.

Microsoft Redefines Gregorian Calendar

According to Microsoft Officials, 10th October 2006 took place on 27th September. Microsoft has committed to scheduling releases of security fixes to the second Tuesday of the month, so the release of two patches (MS06-055 and MS06-049) clearly indicates a jump of thirteen days.

More information:

http://www.microsoft.com/technet/security/bulletin/ms06-049.mspx

http://www.microsoft.com/technet/security/Bulletin/MS06-055.mspx

Zero–Day Word Vulnerability Exploited

On 5th September a zero–day exploit was revealed by Trojan.Mdropper.Q. Symantec has rated the risk as "Very Low". Microsoft did not release a patch on September's scheduled "Patch Tuesday".

More information:

http://www.microsoft.com/technet/security/advisory/925059.mspx

http://www.hkcert.org/salert/english/s060905_msword_codeexe.html

http://secunia.com/advisories/21735/

http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-090219-2855-99

http://www.theregister.com/2006/09/14/ms_patch_tuesday/

Pump and Dump

Pump–and–dump spammers typically buy up cheap stocks, start a massive spam campaign claiming the price is about to rise, and sell the stock when unwise investors follow the "hot lead". Now it appears they are changing tactics, offering to boost the stock price of companies for a fee.

More information:

http://www.theregister.com/2006/09/06/pump-and-dump_spam_tactics/

Zero-Day PowerPoint Vulnerability Exploited

On 18th September, Trojan.PPDropper.E was discovered exploiting a previously unknown vulnerability in Microsoft PowerPoint. Symantec rated the risk as "Very Low".

More information:

http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-091810-5028-99

http://www.hkcert.org/salert/english/s060920_msppt_codeexe.html

http://secunia.com/advisories/22127/

http://www.microsoft.com/technet/security/advisory/925984.mspx

Zero-Day Internet Explorer Vulnerability Exploited

Security researchers at Sunbelt Software discovered a critical problem in Microsoft's implementation of VML being exploited by malicious web sites on 18th September. Microsoft has confirmed the vulnerability.

Interestingly, this may not be a zero-day exploit, when Sunbelt started discussing the exploit, other researchers confirmed that this was the first they had heard of it. However, it later became apparent that ISS had been aware of it for some time, and had been working with Microsoft on a fix. This adds more fuel to the full disclosure debate: ISS and Microsoft denied potential victims the opportunity to take mitigating steps by keeping the exploit secret; or perhaps their actions reduced the number of bad guys that were using the exploit for a while?

Early advice was to mitigate the threat by unregistering the VML dll:

> Click Start, click Run, type
>
> `regsvr32 -u "%CommonProgramFiles%\Microsoft Shared\VGX\vgx.dll`
> and then click OK.

Microsoft released a patch on 27th September.

More information:

http://www.microsoft.com/technet/security/advisory/925568.mspx

http://secunia.com/advisories/21989/

http://www.frsirt.com/english/advisories/2006/3679

http://www.us-cert.gov/cas/techalerts/TA06-262A.html

http://www.hkcert.org/salert/english/s060920_msie_vml.html

http://www.f-secure.com/weblog/archives/archive-092006.html#00000975

http://www.f-secure.com/weblog/archives/archive-092006.html#00000974

http://sunbeltblog.blogspot.com/2006/09/seen-in-wild-zero-day-exploit-being.html

http://sunbeltblog.blogspot.com/2006/09/minor-change-to-vml-exploit-mitigation.html

http://www.microsoft.com/technet/security/Bulletin/MS06-055.mspx

http://www.theregister.com/2006/09/27/ms_emergency_patch/

A New Biometric: Heartbeat-ID?

Proving our identities is difficult, but a company called Thinsia has come up with a novel biometric: your heartbeat. They also have a little story about “Adrian” that illustrates how it will all work. Now let’s take that story a little further…

Adrian Goes Home

> Adrian leaves his desk, and is automatically logged of his computer. In the carpark, his Heartbeat-ID again unlocks the car door automatically. On the way home, he feels unwell, he's having a mild heart attack. He pulls over, stops the car and calls an ambulance. While he's waiting, he opens the window... it doesn't work. It's feeling stuffy, the door won't open either, he's trapped and feels panicy. The extra stress brings on a second, larger heart attack and he dies while the ambulance crew are waiting for firemen with cutting equipment. The body remains unidentified, because Adrian was using his heartbeat as his only form of ID.

OK, a bit melodramatic, but is Heartbeat-ID a good identity system? The PDF linked from the Thinsia site (http://www.pa.icar.cnr.it/IDAschool/lectures/chaos_realworld1.pdf) has this line:

> "*This observed pattern can be modified if pathological heart conditions take place.*"

So, heart disease changes your heartbeat (sounds kind of obvious). Everyone's heartbeat might be unique, but does it have constant elements that can be used for identification? What about other changes to heartbeat - like during exercise? It could be kind of awkward to discover you can't open your car door until you've relaxed for five minutes after running from muggers.

Before deciding that Heartbeat-ID is the perfect biometric, let's have some traditional measures of reliability: false positives, and false negatives. What is the protection against replay attacks (record someone's heartbeat, replay it to the Heartbeat-ID watch)? Are there vulnerabilities in the implementation: e.g. could someone build a Heartbeat-ID watch that can produce a fake, variable signal (keep varying the signal until the lock opens - just like password guessing)?

There are questions about Adrian's seamless experience too... Is it really practical, e.g. how do you ask a friend to open the door for you when your hands are full? Is this the new Big Brother – total monitoring of people's every move and action? If extremists got access to the central database, they could target people by beliefs or affiliations extremely efficiently!

Any claim that a new authentication or identification method will solve all our problems is likely to be bogus. Different applications require different characteristics: you want to know that the person accessing your database is alive, but dental records are far more useful in grimmer circumstances.

More information:

http://www.thinsia.com/adrian.html

http://www.thinsia.com/products/heartbeat-id.html

http://www.pa.icar.cnr.it/IDAschool/lectures/chaos_realworld1.pdf

http://cytrap.eu/blog/?p=38

F-Secure Opens Malaysian Lab

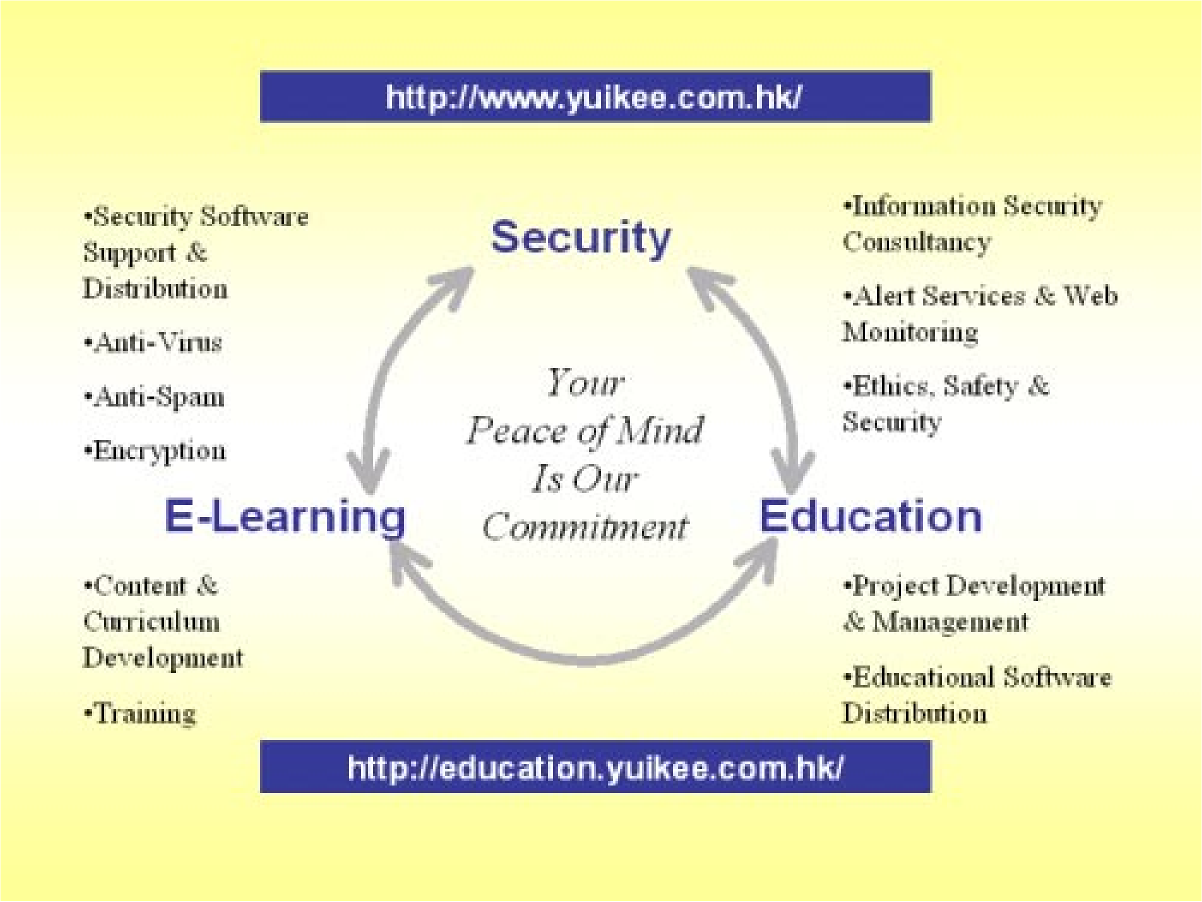
F-Secure has opened their Asian Technology Centre in Kuala Lumpur. This will act as their Asian headquarters, and the location of their Security Labs. Malware analysis will be split between Finland and Malaysia.

More information:

http://www.f-secure.com/weblog/archives/archive-092006.html#00000969

YUI KEE
鋭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: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/



http://www.yuikee.com.hk/

Security

- Information Security Consultancy
- Alert Services & Web Monitoring
- Ethics, Safety & Security

Education

- Project Development & Management
- Educational Software Distribution

E-Learning

- Content & Curriculum Development
- Training

- Security Software Support & Distribution
- Anti-Virus
- Anti-Spam
- Encryption

Your Peace of Mind Is Our Commitment

http://education.yuikee.com.hk/