Yui Kee Computing Ltd.

Newsletter

October 2007

Contents

Contents.. 1
F-Secure Slams Mobile-Spy's Lax Security.. 1
Kaspersky Lab's Virus Top Twenty for September 2007 1
10th AVAR Conference in Seoul 3
Asia Pacific's first HTCIA Training Conference... 3
Humour: Bobby Tables 4
Phishing Site Hosted on Police Server 4
Anonymity and Secrecy: Why Sin Chung Kai Should Apologise 4
MP3 Spam Off to a Slow Start 5
Adobe Acrobat Vulnerability Exploited in spam 5

F-Secure Slams Mobile-Spy's Lax Security

<web-link for this article>

F-Secure has said that Retina-X Studios' Mobile Spy is "not built to be secure". Mobile Spy is an application aimed at businesses wishing to ~~spy on~~ monitor their employees' Windows Mobile smartphone traffic. In a posting on their weblog, F-Secure revealed how the Mobile Spy website could be made to display call details for other accounts simply by changing the account ID in the URL, up until a couple of days before the public announcement of the flaw.

In a statement, James Johns, Retina-X Studios chief executive, claimed that the flaw did not exist, and all their servers had been tested for it.

F-Secure later reported that, although the original flaw had been fixed, they had received reports that the server was vulnerable to SQL injection attack, so all Mobile Spy's customer's data was potentially still at risk.

More Information

Leaky Spy Tools?

F-Secure slams mobile spying application

F-Secure attacks smartphone spying software

Kaspersky Lab's Virus Top Twenty for September 2007

<web-link for this article>

Russian anti-virus developer Kaspersky Labs has published their statistics of the most prevalent viruses in September 2007. They noted that their predictions for September were not entirely accurate, with all Warezov variants dropping of the Top Twenty list, and Netsky.q, in first place again, has become the most widespread malicious program in the history of the Internet.

Position	Change in position	Name	Percentage
1	-	Email-Worm.Win32.NetSky.q	25.22%
2	+1	Email-Worm.Win32.NetSky.aa	10.83%
3	+3	Email-Worm.Win32.Mydoom.l	10.04%
4	-2	Email-Worm.Win32.Bagle.gt	7.62%
5	Return	Email-Worm.Win32.Nyxem.e	6.03%
6	-2	Net-Worm.Win32.Mytob.c	5.18%
7	-2	Worm.Win32.Feebs.gen	4.69%
8	-1	Email-Worm.Win32.NetSky.t	3.03%
9	New	Trojan-Spy.HTML.Paylap.bg	2.62%
10	-	Email-Worm.Win32.NetSky.b	2.62%
11	-	Email-Worm.Win32.NetSky.x	2.35%
12	-	Email-Worm.Win32.Scano.gen	1.72%
13	-5	Exploit.Win32.IMG-WMF.y	1.58%
14	-5	Net-Worm.Win32.Mytob.t	1.38%
15	+3	Net-Worm.Win32.Mytob.dam	1.35%
16	-	Email-Worm.Win32.Womble.a	1.06%
17	Return	Email-Worm.Win32.NetSky.d	1.03%
18	-5	Net-Worm.Win32.Mytob.u	0.97%
19	Return	Email-Worm.Win32.Mydoom.e	0.93%
20	Return	Email-Worm.Win32.NetSky.y	0.83%
		Other malicious programs	8.92%

More Information

Virus Top 20 for September 2007

Online Scanner Top Twenty for September 2007

10th AVAR Conference in Seoul

<web-link for this article>

The tenth Anti-Virus Asia Researcher's Annual Conference will be held at the Seoul Plaza Hotel from the 28th to 30th November 2007. This is the third time the AVAR Conference has been held in Korea.

AVAR is a non-profit organization whose primary objective is to prevent the spread and the damage caused by malicious code. AVAR now comprises members from 15 countries/regions, not just from the Asia pacific area, but from all over the world. AVAR is not only a conference for virus researchers, but also for corporate IT professionals, students, educators, law enforcement, legislators, and all who work toward the goals of safe computing and the secure internet.

The conference program includes presentations from many of the leading anti-virus developers and researchers, and government agencies. Yui Kee's Chief Consultant will be presenting a paper on Hong Kong's anti-spam legislation.

More Information

AVAR 2007 Conference in Seoul

Conference Programme

Conference Registration

Asia Pacific's first HTCIA Training Conference

<web-link for this article>

The Asia-Pacific Chapter of the High Technology Crime Investigation Association (HTCIA) will hold it's first Training Conference from Wednesday 12th to Friday 14th December 2007. This is in line with their commitment to bring the highest quality hands-on training in cybercrime investigation and computer forensics to the Asia Pacific Region.

The conference includes a one-day Management Track a two-day Presentations Track and three three-day tracks of hands-on training from some of the best-known names in investigations and forensics. Speakers include (subject to possible late changes):

Brian Carrier—Author of “File System Forensics” and creator of open source forensic tools Sleuthkit and Autopsy

Harlan Carvey—Author of “Windows Forensic Analysis” and acclaimed expert on Windows Registry Forensics

Andrew Rosen—Original author of Expert Witness (now known as EnCase) and author of the Linux forensic tool SMART

Stefan Fleischmann—Author of widely used tools Winhex and X-Ways Forensics

Michael Cohen—Author of open source forensic tool PYFlag

Kevin Mansell—Leading UK LE trainer in the field of mobile device forensics

Plus a whole host of regional experts in the fields of Malware analysis, Incident Re-sponse, Hacking Investigation and much more...

More Information

2007 HTCIA Asia Pacific Training Conference

Humour: Bobby Tables

<web-link for this article>

A hilarious cartoon for anyone writing input validation code.

I hear that Bobby Tables found this all a little bothersome, so he changed his name when he left College... to Robert'); DROP TABLE Employees;

Technical note: this website is updated via a web-form inputting data to a SQL database. As you are reading this article, it is safe to say that the input data is correctly handled.

More Information

Exploits of a Mom

Phishing Site Hosted on Police Server

<web-link for this article>

A server at the Sardar Vallabhbhai Patel National Police Academy (SVPNPA) in India was spotted hosting a phishing site for the Bank of America. The site has now been shut down, and an official at the SVPNPA has confirmed the incident and said that an investigation is under way.

The Academy provides courses on computer crime. Now they will have an interesting case-study for their courses.

More Information

Police Academy in India Hosting a Phishing Site

Hackers phish Americans through Police Academy website

Hackers phish Americans through Police Academy website

Politiskole brukt av phishere

Anonymity and Secrecy: Why Sin Chung Kai Should Apologise

<web-link for this article>

Anonymity and privacy are not the same: when you walk down the street you are in the public view but you are a "face in the crowd", fairly anonymous. You can increase your anonymity, say by wearing a mask (*I have an infectious disease today...*) but what you are doing is still completely public. Conversely, voting is different: the polling station staff record your identity, in Hong Kong that will be verified with your ID card, but how you vote is entirely private.

The same applies on the Internet, which brings us to the case reported in this newsletter last month where Swedish security researcher Dan Egerstad published a list of one hundred passwords of government-related email accounts, including Legislative Council members. Mr. Egerstad has now revealed how he did it. He set up five ToR exit nodes, at different locations in the world, equipped with a custom packet-sniffer focused entirely on POP3 and IMAP traffic using a keyword-filter looking for interesting government-related domains.

Tor is a network of virtual tunnels that allows people and groups to improve their anonymity on the internet. A user can install a Tor client and their traffic will be fed through a network of Tor nodes before exiting to the ordinary internet to reach its destination. No node will know both the source and destination. There are many valid uses for Tor, groups like the Electronic Frontier Foundation (EFF) recommend it for maintaining civil liberties online.

What Tor cannot do is protect the communication after it has left the network; the exit node, and anyone along the route that the traffic takes to its destination, can examine the contents. If the contents are an unencrypted POP3 or IMAP session, that includes your email address and password, which completely undermines the anonymity provided by Tor. The Tor developers are completely open about this limitation, and recommend end-to-end to deal with it. The users whose account details were revealed by Mr. Egerstad ignored this advice. RTFM (Read The *Friendly* Manual).

On 5th September 2007, one of the people who used Tor without reading the manual, Hon. Sin Chung Kai, wrote of Mr. Egerstad, "I seriously condemn the hacking activities of this person. His attack to the network likely constitutes a violation of Hong Kong laws, such as Telecommunication Ordinance (Chapter 106) Section 27A Unauthorized access to computer by telecommunications; Crimes Ordinance (Chapter 200) Section 161 Access to computer with criminal or dishonest intent, etc, which can lead to criminal liability." From the details revealed by Mr. Egerstad, it is clear that there was no unauthorised access to a computer, and no apparent criminal or dishonest intent. Perhaps Hon. Sin would like to withdraw his accusation and apologise to Mr. Egerstad?

More Information

Tor: Overview

Can exit nodes eavesdrop on communications? Isn't that bad?

Hong Kong Liberal Party Can Count but Sin Chung Kai uses Wife's Name in Password

Anonymity and the Tor Network

Lesson From Tor Hack: Anonymity and Privacy Aren't the Same

Phishing attacks on Tor anonymisation network

Embassy leaks highlight pitfalls of Tor

Time to reveal…

Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise

MP3 Spam Off to a Slow Start

<web-link for this article>

Predictions that MP3 files will be used to carry spam messages to avoid current filtering techniques have been proved true by the first mass mailing of a stock pump-and-dump scam. The file features a female voice promoting the stock of a Canadian car trading company. However, the expert consensus is that the limitations of MP3 will make it unsuccessful for spammers.

More Information

Kaspersky Lab detects the first mass mailing of MP3 spam

Stock spammers pump up the volume with MP3 files

Pump-and-dump scammers debut MP3 spam

MP3 spam

Adobe Acrobat Vulnerability Exploited in spam

<web-link for this article>

A malicious PDF file was been massively spammed through e-mail. The crafted PDF file used a vulnerability related to the mailto: option and Internet Explorer 7 on Windows XP, Mitre exploit CVE-2007-5020 to download and execute ms32.exe, which downloaded further components. The secondary download location was swiftly shut down, preventing major problems.

More Information

Malicious PDF Files Being Spammed Out in Volume

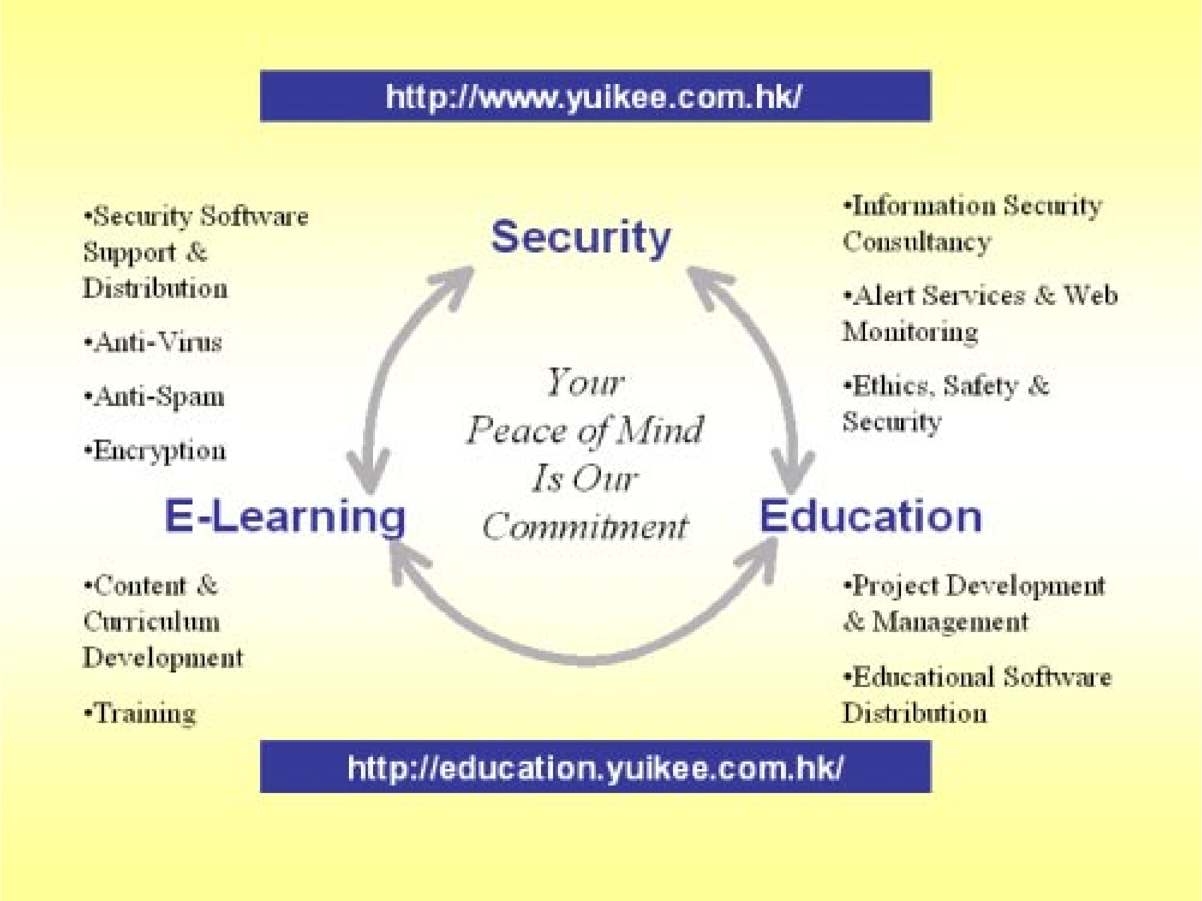
Report: PDF files used to attack computers

CVE-2007-5020

Microsoft confirms PDF attacks, urges caution

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



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

Security

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

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

Your Peace of Mind Is Our Commitment

E-Learning

- Content & Curriculum Development
- Training

Education

- Project Development & Management
- Educational Software Distribution

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