Yui Kee Computing Ltd.

Newsletter

September 2008

Contents

Inheritance Spammer Jailed in Hong Kong

<web-link for this article>

On 9th September, a District Court in Hong Kong convicted a 34-year-old man to 3 years jail for money laundering. The offender came to Hong Kong in 2007 and, using his real name, set up bank accounts in the names of three companies where he was sole Director. He then sent out classic Advanced Fee Fraud (AFF) emails, saying he needed assistance in transferring money left by a deceased foreigner. A male victim initially believed the story, and sent the various "administrative fees" requested, but later felt suspicious and contacted the Police.

The Fraud Division of the Commercial Crime Bureau in Hong Kong investigated and discovered that large sums of overseas remittances were conducted between March to October 2007 through the bank accounts. The offender was arrested in October last year and later charged with money laundering. He was convicted of three counts.

Police appealed to the members of the public to be cautious when they receive any unsolicited offers by means of promising rewards on payment of any advanced fee. The public is strongly advised not to respond to such offers and anyone who has come across such similar suspected fraud cases are advised to make a report to the Police.

More Information

Man jailed for money laundering
Man jailed for money laundering via email in Hong Kong

SSH Tectia® Certified With RSA Secured® Partner Program

<web-link for this article>

SSH Communications Security Corp., a world-leading provider of enterprise security solutions and end-to-end communications security, and the original developer of the Secure Shell protocol, today announced it has joined the RSA Secured® Partner Program and certified interoperability between the SSH Tectia Client/Server and SSH Tectia ConnectSecure™ from SSH Communications Security and both the RSA® SecurID and RSA® Certificate Manager

solutions from RSA, The Security Division of EMC. SSH Communications Security believes that its enterprise customers will benefit from this interoperability partnership through enhanced data security, reduced deployment time and lower overall cost of ownership.

Together, SSH Tectia and RSA SecurID help to protect mission-critical file transfers and data-in-transit with two-factor authentication for secure access control and a more reliable chain of custody. RSA Certificate Manager is engineered to provide a scalable system that automates and centralizes the management of cryptographic keys and digital certificates.

“It is more critical than ever for companies to increase the security and integrity of their valuable information. In order to help our joint customers better protect their information, we are pleased to be working with SSH Communications Security to achieve interoperability between RSA technology and SSH Tectia Client/Server and SSH Tectia ConnectSecure,” said D.J. Long, senior director, Corporate Development at RSA. “Our organizations are committed to help mitigate risk to sensitive information throughout its lifecycle to ensure that it is always an asset, and not a liability, and allows organizations to accelerate their business objectives.”

SSH Tectia Client/Server is the de facto standard enterprise security solution used by millions worldwide for secure file transfers, system administration and application connectivity throughout the network. SSH Tectia provides transparent, strong encryption, flexible authentication options, direct support for all major industry platforms, and superior performance, without requiring modifications to the existing infrastructure or applications. It also helps organizations meet regulatory compliance requirements, including the Federal Information Processing Standards (FIPS) 140-2 certified cryptographic algorithm for use in U.S. federal government applications. In addition, the commercially supported SSH Tectia solution with SSH Tectia Manager helps enterprises achieve compliance with PCI DSS and other government regulatory requirements.

The award-winning SSH Tectia ConnectSecure enables organizations to quickly and cost-effectively secure any File Transfer Protocol (FTP) file transfer and data-in-transit without any modification to the existing infrastructure, scripts or applications, and is compatible with any commercial SSH or OpenSSH environment.

The SSH Tectia solution, which includes SSH Tectia Client, Server, Manager, ConnectSecure, and Server for IBM z/OS, allows enterprises to implement high-performance secure file transfers, secure application connectivity and secure system administration throughout heterogeneous networks. SSH Tectia ConnectSecure provides revolutionary features, including automatic FTP-to-SFTP conversion, transparent FTP, and TCP/IP application tunneling to quickly replace unsecure protocols with secure ones. SSH Tectia ConnectSecure significantly increases the number of enterprises, financial institutions, major retailers, and government agencies that can leverage its cost-saving benefits. “Many of the world’s largest enterprises and government agencies have come to rely on SSH Tectia to secure even their most sensitive company and consumer data,” said George Adams, CEO, SSH Communications Security, Inc. “By providing interoperability with leading digital certificate management and authentication solutions, we are offering joint customers an unmatched level of data security and an additional layer of powerful protection for key corporate assets.”

Lessons from Sarah Palin's Email Exposure

<web-link for this article>

Allan Dyer

Reports indicate that U.S.A. Vice-Presidential Candidate Sarah Palin's webmail account was broken into by means of Yahoo's password recovery facility. A person using the handle, "rubico" claims to have researched the answers to the security questions in 45 minutes on the internet. The required information was:

- Birthday
- Zip code
- “Where did you meet your spouse?”

The contents of Sarah's email may or may not be interesting or important to Americans considering their country's future, but the first lesson for everyone is the weakness of self-service password reset procedures. The supposedly "secret" information in this case are things that can be easily revealed for anyone with on online presence, or friends with an online presence. Even if you have a cast-iron rule to not reveal your birthday, a friend might blo9g about enjoying your party last week, or give clues to any other personal question. As I pointed out in the May issue of this newsletter, 'Personally, any information about me that is memorable and I would be willing to tell to a website is probably not a secret, and if it is not memorable, I won't remember it either, making it useless as a "security question".'

The second lesson is that webmail services like Yahoo have very little obligation to protect your information. Yahoo is not going to shut down and improve its security because of this incident, there are, undoubtedly, many other similar incidents occurring daily that do not hit the headlines because they do not involve a famous person. If you do not chose "security questions" that are difficult to guess or research, then, from Yahoo's point of view, that is your fault.

The third lesson is for the attackers: if you break into the account of someone famous, be prepared for some serious trouble. The FBI wants to talk to "rubico", and they have the resources to trace the source. A quick confession might be forthcoming, Democratic state Representative Mike Kernell, from Tennessee, told a reporter with the Tennessean that his 20-year-old son, David, is the individual involved.

Email is not secure. Webmail is even less secure. Use with caution.

23rd September 2008

FBI Gatecrashes Student Party

FBI officers searched the flst of David Kernell, a suspect in the Sarah Palin webmail hack case, in the early hours of Sunday morning, interrupting a student party. Kernell was not present, but his three flatmates were served with court summons. Guests who did not live in the flat were asked to wait outside while officers photographed the flat. Strangely, there was no mention of computer equipment being seized. The raid follows an earlier FBI visit on Friday afternoon.

More Information

Security researchers ponder possible Palin hacks
Anonymous hacks Sarah Palin's Yahoo! account
How a b-tard hacked Sarah Palin's Yahoo account
The story behind the Palin e-mail hacking
Identity of Palin Hacker discovered? Rubico may be the culprit
Web proxy firm working with FBI to trace Palin e-mail hacker
Questioning Password Resets
Democratic rep fathered alleged Palin hacker
Palin E-Mail Hacker Says It Was Easy
Feds search Palin hack suspect's flat
Police Raid Apartment of David Kernell in Sarah Palin's Yahoo Email Hack
FBI Agents Raid Campus Apt. of Alleged Palin Hacker

Hong Kong Police use Microsoft's COFEE Live Forensic Tool

<web-link for this article>

Speaking in an interview with ZDNET, Chief Inspector Paul Jackson of the Technology Crime Division, Hong Kong Police Force, revealed the force's use of a beta version of COFEE. COFEE (Computer Online Forensic Evidence Extractor) is a live forensics tool developed by Microsoft that automates the use of 150 evidence-gathering commands. Available only to law enforcement agencies, the beta version of COFEE was released earlier this year and, Jackson revealed, initial used by the Hong Kong Police in "incidence response" situations.

The developer of the tool, Anthony Fung, Microsoft's senior regional manager for Internet safety and anti-counterfeiting in the Asia-Pacific region, stressed that COFEE is meant to complement existing tools and is not a silver bullet. Jackson confirmed that investigators do not depend solely on COFEE but also use other tools for validation.

Fung reported that the beta phase has closed and Microsoft will release COFEE once the legal logistics are complete.

More Information

Hong Kong police gets Cofee boost

Security Company Hijacks Brad Pitt's name for Marketing

<web-link for this article>

In a cynical marketing move, McAfee has named Brad Pitt as the Most Dangerous Celebrities in Cyberspace. In a press release that drips with celebrities' names, including Paris Hilton, Beyonce, Justin Timberlake and Heidi Montag, the company reports on data from its SiteAdvisor technology that, it claims, show that user searching for "Brad Pitt" and variants have an 18% chance of having their PCs infected with online threats, such as spyware, spam, phishing, adware, viruses and other malware.

Like McAfee's "Mapping the Mal Web" report, discussed in our June issue, the latest release also tries to attract attention by hyping unimportant details in a way that misleads ordinary readers. Paul Ducklin of Sophos criticises McAfee for failing to point out that malware-infected websites have a huge variety of themes, "The story seems to imply that if you steer clear of celebrities and stick to 'safer' subjects, you will greatly improve your online health. But SophosLabs finds an average of about 16,000 newly-infected web pages per day, liberally distributed throughout cyberspace".

Editor's note: in a cynical move to improve user education, this article uses celebrity names to attract attention. I hope you approve.

More Information

McAfee, Inc. Names Most Dangerous Celebrities in Cyberspace
"Mapping the Mal Web" is the New "Virus Calendar"
Brad Pitt Tops Charts For Most Celebrity Malware Sites
Brad squeezes Paris out of unsafe search chart
Brad Pitt named as top malware lure

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/