Yui Kee Computing Ltd.

Newsletter

February 2010

Contents

Hongkong Post e-Cert Subscribers Told Certificates Expired

<web-link for this article>

About 11am on 9th February, Hongkong Post e-Cert sent email Suspension Notices to all holders of expired e-Certs, including those who also held currently-valid e-Certs, causing confusion, and flooding their hotline with calls.

Hongkong Post is a recognised Certification Authority under Hong Kong's Electronic Transaction Ordinance, which gives digital signatures supported by an e-Cert the same legal status as a handwritten signature. As a public CA, Hongkong Post CA issues recognised digital certificates to individuals and corporations. The certificates have a valid lifespan, of one or more years, when they can be used for signing. Naturally, Hongkong Post retains records of expired certificates - the signatures created during the lifespan of the certificate are still valid, even though the certificate can no longer be used for creating new signatures.

Normally, Hongkong Post sends email reminders to certificate holders about the time their certificate is going to expire. For reasons as yet unexplained, Hongkong Post sent reminders for all expired certificates. The messages did clearly indicate the Subscriber Reference Number and Certificate Serial Number, so it was possible for subscribers to identify that the message referred to an old certificate, not the current certificate the subscribers were using.

We are awaiting further information on this incident from Hongkong Post.

24th February 2010

Emily Wong of E-Mice Solutions (HK) Limited, the operator of HKPost e-Cert services, has responded in two emails. Ms. Wong confirmed that a computer-generated "Suspension Notice" was scheduled and released on 8 - 9 February 2010 and therefore the call volume of the e-Cert service hotline was, "a bit higher than normal days as we expected", without specifying the normal call volume, or the size of the spike in demand.

Ms. Wong also explained that this was not an incident - in the instance of Mr. Dyer's certificate, they had, in accordance with their operation procedures, sent a "Subscription Expiry Notice" on 22/04/2008, one month before the expiry date. The "Suspension Notice" sent on 9th February 2010 was a reminder of the suspension, and an explanation of how to reactivate the suspended e-Cert for use, until its final expiry on 22/05/2010.

Ms. Wong emphasised that security was not compromised, "HKPost CA always uses a trustworthy system for the issuance, revocation or suspension, and publication in a publicly

available repository of accepted recognized certificates. Further details are disclosed in the e-Cert Certificate Practice Statement ("CPS")".

Our Chief Consultant, Allan Dyer, commented, "This still leaves questions unanswered, why was a Suspension Notice sent 628 days after the suspension, and only 102 days before the certificate expired? I did find it difficult to contact a hotline operator on 9th February, and the impression I received when talking to the operator was that the lines were flooded, so what were the figures, and, if this was an expected increase, why weren't more resources allocated for the period?" Reviewing the surrounding circumstances, Dyer made some recommendations:

1. Avoid confusing and inconsistent terminology in notices. The "Subscription Expiry Notice" says, "the first-year subscription period of your e-Cert is about to expire", but later says, "your e-Cert will be suspended and published on the Certification Revocation List to indicate that your e-Cert has ceased to be valid". Valid, invalid, expired, and suspended have closely-related meanings in English, but a suspension is usually temporary, expiry is normally permanent. The confusion is not helped by the varying terminology used in browsers, Internet Explorer reports that certificates are "Valid from" and "Valid to", Firefox specifies their "Validity" as "Issued On" and "Expires On". Sending out a expiry notice when a certificate is about to be suspended might lead a user to apply for a new certificate when their current certificate could still be renewed.
2. Simplify notices by omitting irrelevant material. The Expiry notice also says, "If you are a subscriber of e-Cert (Personal / Minor), you have to apply for e-Cert (Personal) and stop using e-Cert (Personal / Minor) when you aged 18", but this is only needed in notices sent to people about to turn 18. Filling the notice with irrelevances increases the possibilities of users missing important details.
3. Keep your customers. The information for people turning 18 continues, "The residual subscription period of the e-Cert (Personal / Minor) will become invalid", why not allow a free upgrade for the remainder of the certificate period?
4. Review the timing of notices, especially the Suspension Notice. Is there any point in sending the Suspension Notice 628 days after the date the certificate was suspended, inviting the user to renew the certificate for the remaining 102 days until the certificate expires, at a cost of $100, when the user can apply for a new certificate, valid for a full year, for just $50?

More Information

Hongkong Post e-Cert
Hongkong Post 香港郵政

Microsoft Cuts Waledac Botnet

<web-link for this article>

Following the grant of a temporary restraining order by a US Judge on 22nd February, Microsoft has taken action, known internally by the codename "Operation b49", to disable the Waledac botnet. The action includes de-registering 277 domains, and unspecified "additional technical countermeasures" to downgrade the peer-to-peer communications between infected computers. The 277 domains are hard-coded into the malware, and are used to contact command-and-control servers.

Criminals design modern malware, like Waledac, with business continuity (or should that be crime continuity?) in mind. The infected computers normally receive commands via their peer-to-peer network, but will contact command-and-control servers (usually also infected computers) via the hard-coded domain names when they have difficulty with their peer-to-peer

network. Cleaning individual computers, or even thousands of computers, has little effect on the overall effectiveness of the botnet, as the remaining hundreds of thousands of infected computers simply re-establish their peer-to-peer network automatically. De-registering the command-and-control domains on its own is also ineffective, as the peer-to-peer network remains, allowing the botnet to be updated with new command-and-control domain information. Thus, simultaneous attack, disabling the domains and disrupting peer-to-peer communications, is necessary to fragment the network beyond repair.

The Waledac botnet is thought to be one of the ten largest botnets, and is implicated in sending spam, DDoS attacks, click fraud and malware distribution. It might be responsible for about 1% of spam emails.

However, Microsoft's actions are not entirely uncontroversial, de-registering domains is an established technique to foil criminals, but disrupting the peer-to-peer communications could be seen as an attack on the computers of innocent victims of the botnet. Charlie Campbell has likened the legal power to a government granting letters of marque and reprisal to privateers. This comparison may not be justified, to speculate, an easy way for Microsoft to disrupt peer-to-peer communication throughout the botnet would be to utilise Windows Update, perhaps to block the ports used by the malware. In this scenario, Microsoft would already have permission from the legal owners of the computers, by the Windows Update EULA. The expected response by criminals would be to disable Windows Update when their malware is installed.

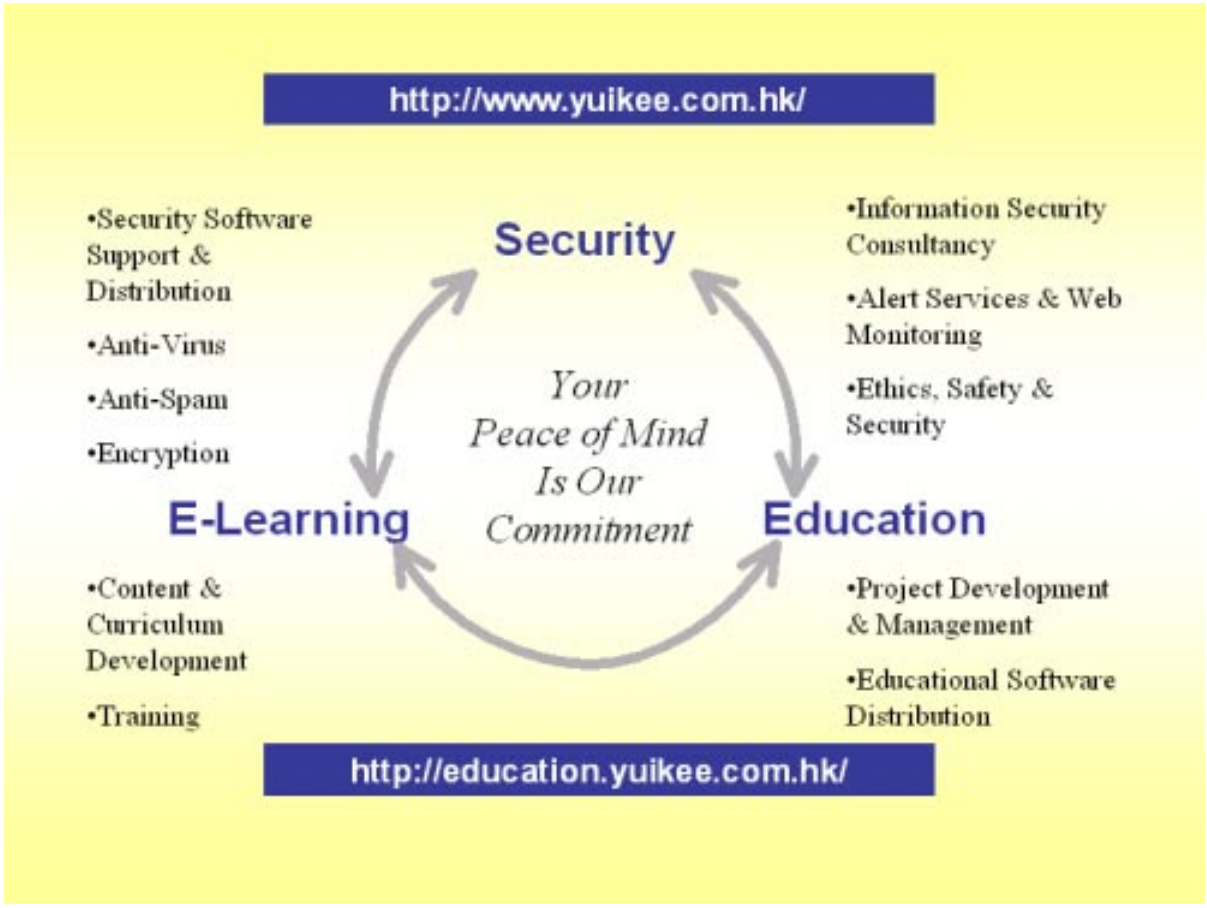
Allan Dyer, our Chief Consultant, commented, "Microsoft has taken a bold step to disrupt this botnet, but we can expect the criminals to adapt quickly. We need to track down the people behind these botnets, and put them away".

More Information

R.I.P. Waledac?
Microsoft wins legal battle against spammers
Microsoft shuts down global spam network
Microsoft's foiling of botnet gets mixed response
The Microsoft Cyber Army & the Judicial Power to Declare War
Cracking Down on Botnets
Microsoft's Complaint
MS uses court order to take out Waledac botnet

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
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/