Security Revolution Analysis Network

Spyware Document

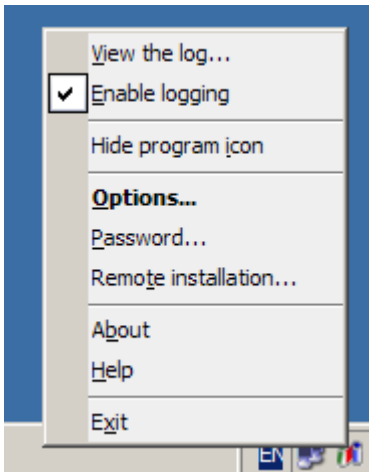
Kiattisak Somwong (Senior Open Source Security Engineer)
Globaltech Company

ตัวอย่างการใช้งานโปรแกรม Perfect Keylogger

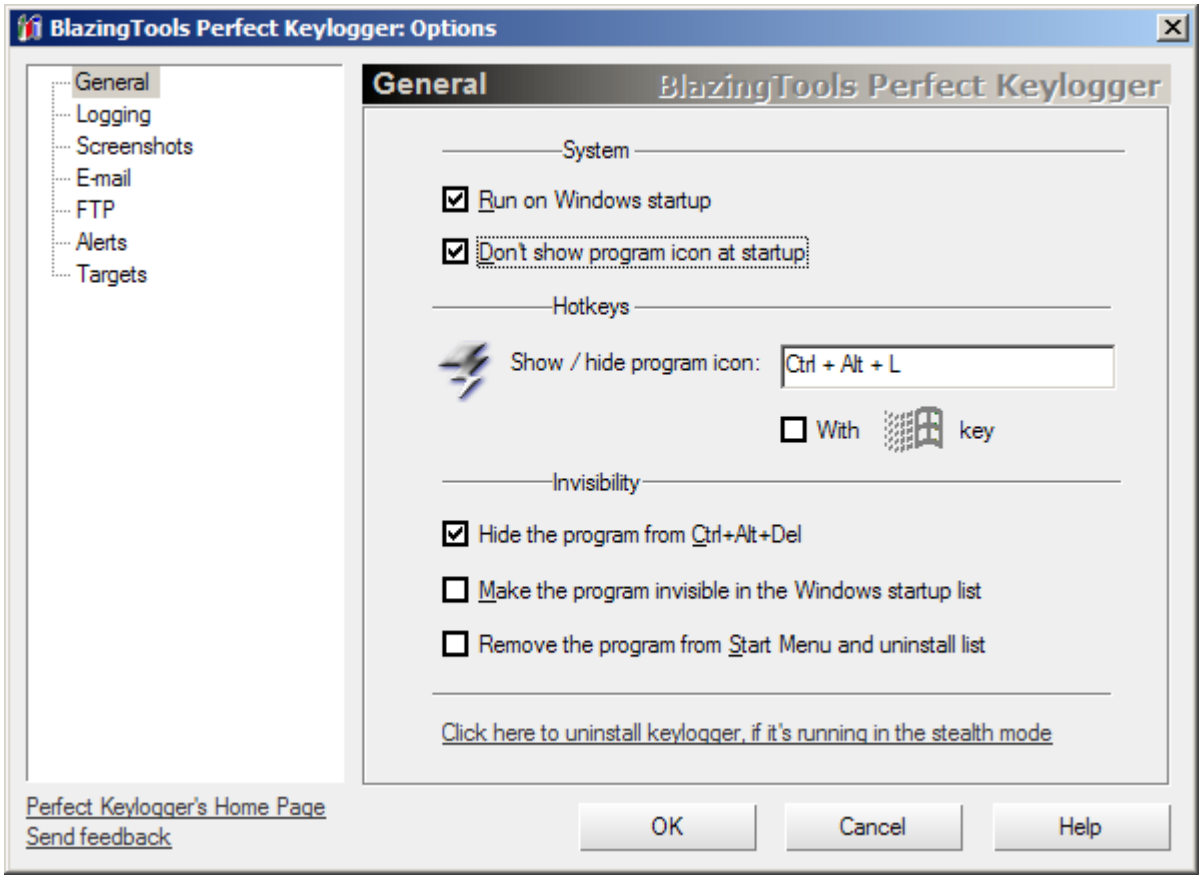
เมื่อติดตั้ง Perfect Keylogger แล้วจะปรากฏภาพไอคอนที่ system tray ดังรูป

เมื่อคลิกขวาที่ไอคอนจะเห็นเมนูดังภาพข้างล่าง

Global Technology Integrated Co.,Ltd.
99/349 Moo 2, Chaengwattana Rd., Tungsonghong, Laksi, Bangkok 10210
Tel : 0 2982 3338-9 , Fax : 0 2982 3338-9 ext. 11
www.gbtech.co.th



จากนั้นจึงคลิกที่ **Options** จะปรากฏหน้าต่างดังข้างล่างนี้

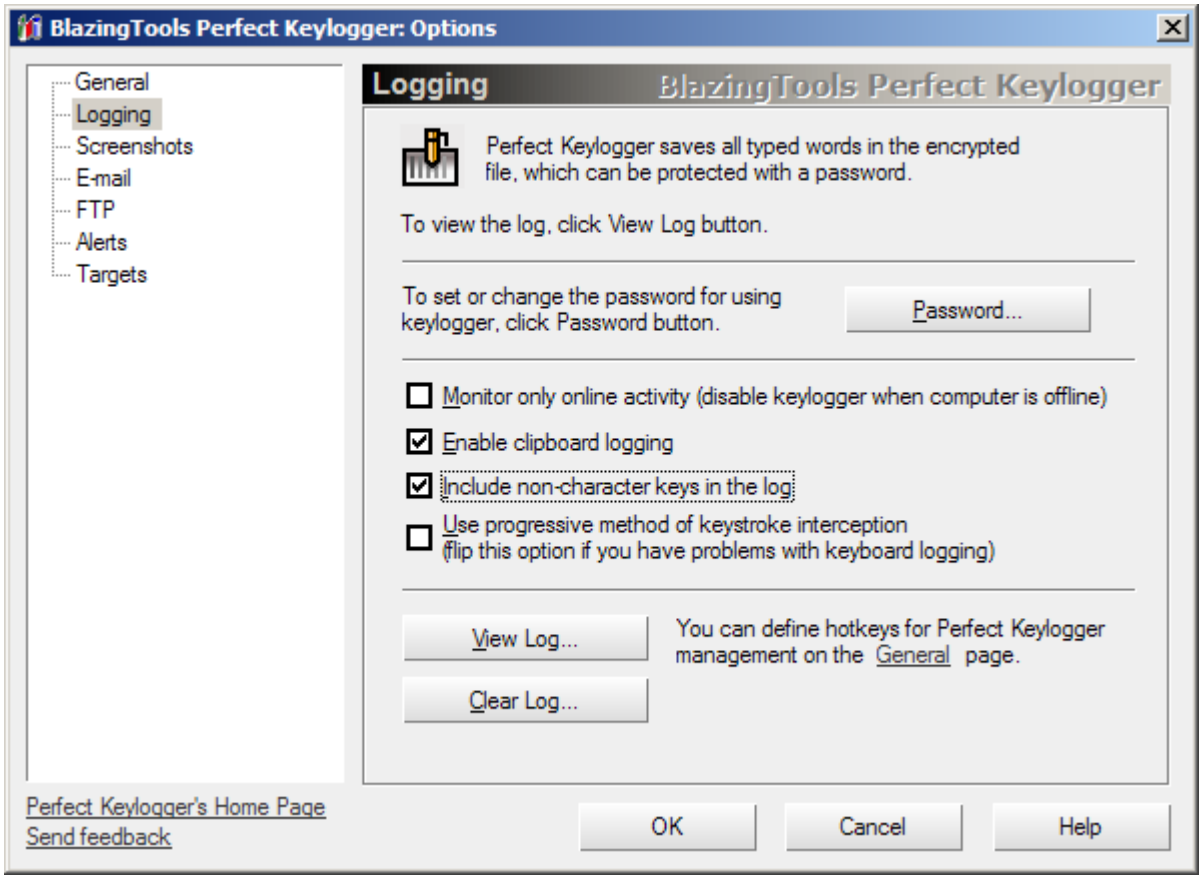


99/349 Moo 2, Chaengwattana Rd., Tungsonghong, Laksi, Bangkok 10210

Tel : 0 2982 3338-9 , Fax : 0 2982 3338-9 ext. 11

www.gbtech.co.th

จากนั้นจึงคลิกที่ **logging** ทางด้านซ้าย แล้วเลือกที่ **Enable clipboard logging** และ **Include non-character keys in the log** (ถ้ามีปัญหาในบันทึกการกดคีย์บอร์ด ให้เลือกที่ **Use progressive method of keystroke interception** ด้วย)



จากนั้นจึงคลิกที่ไปที่หัวข้อ E-mail ถ้าต้องการให้ส่งทางอีเมล ให้เลือกที่ **Try to send logs by e-mail every _ hours _ minutes** โดยใส่เวลาที่ต้องการไปในช่องว่าง ถ้าต้องการให้ key logger ส่ง screenshort ด้วย เลือกที่ **Visual log (screenshorts)**

ส่วน Log file format ให้เลือกเป็น **HTML** แทน เนื่องจากมีความสะดวกในการรับทางอีเมลมากกว่า แต่ถ้าเลือกเป็นแบบ Encrypted ก็จะทำให้ผู้ที่ดักข้อมูลโดยใช้ sniffer หรือ IDS ไม่สามารถอ่านข้อความที่ส่งไปโดย key logger ได้ แต่จะอ่านได้จาก log viewer ของโปรแกรม Perfect Keylogger เท่านั้น

เราสามารถกำหนดให้ key logger ส่ง log เมื่อไฟล์ log มีขนาดตรงที่กำหนดไว้โดยเลือกที่ **Send**

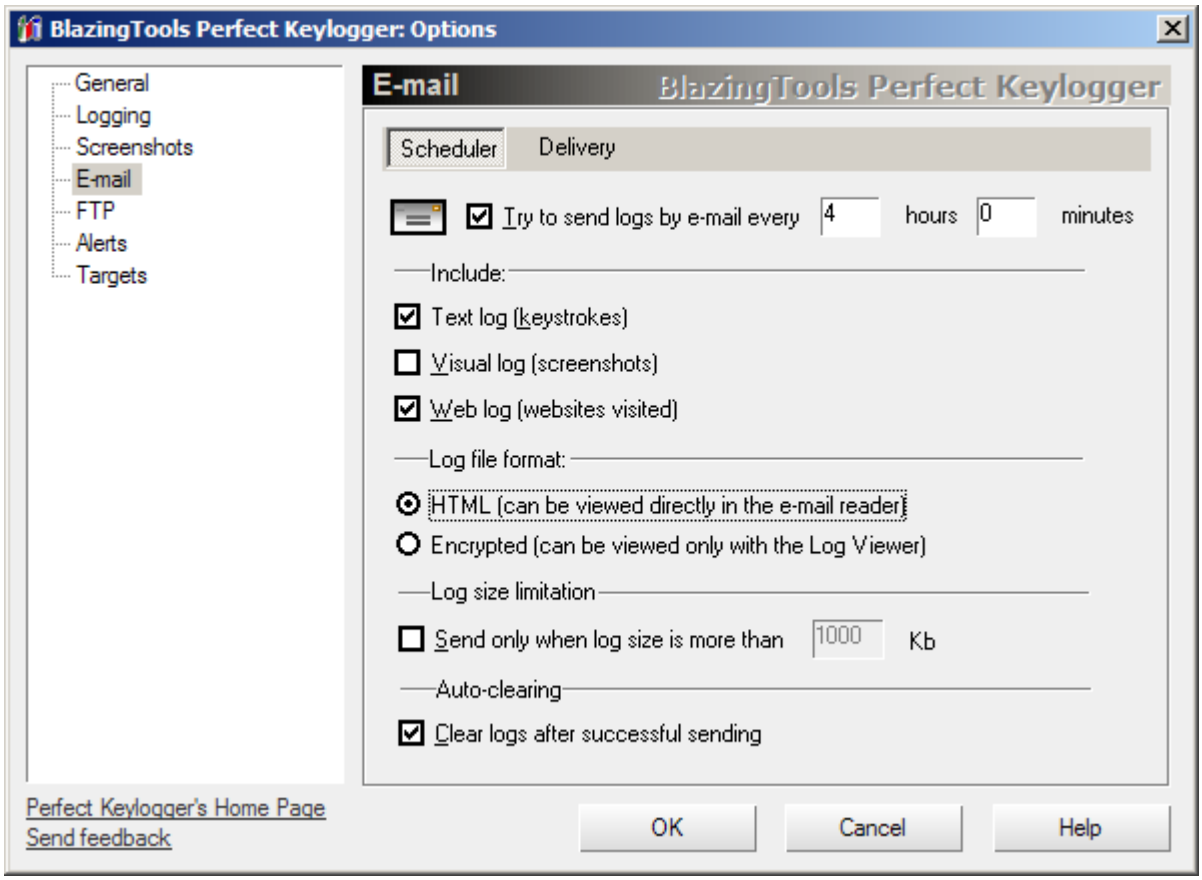
99/349 Moo 2, Chaengwattana Rd., Tungsonghong, Laksi, Bangkok 10210

Tel : 0 2982 3338-9 , Fax : 0 2982 3338-9 ext. 11

www.gbtech.co.th

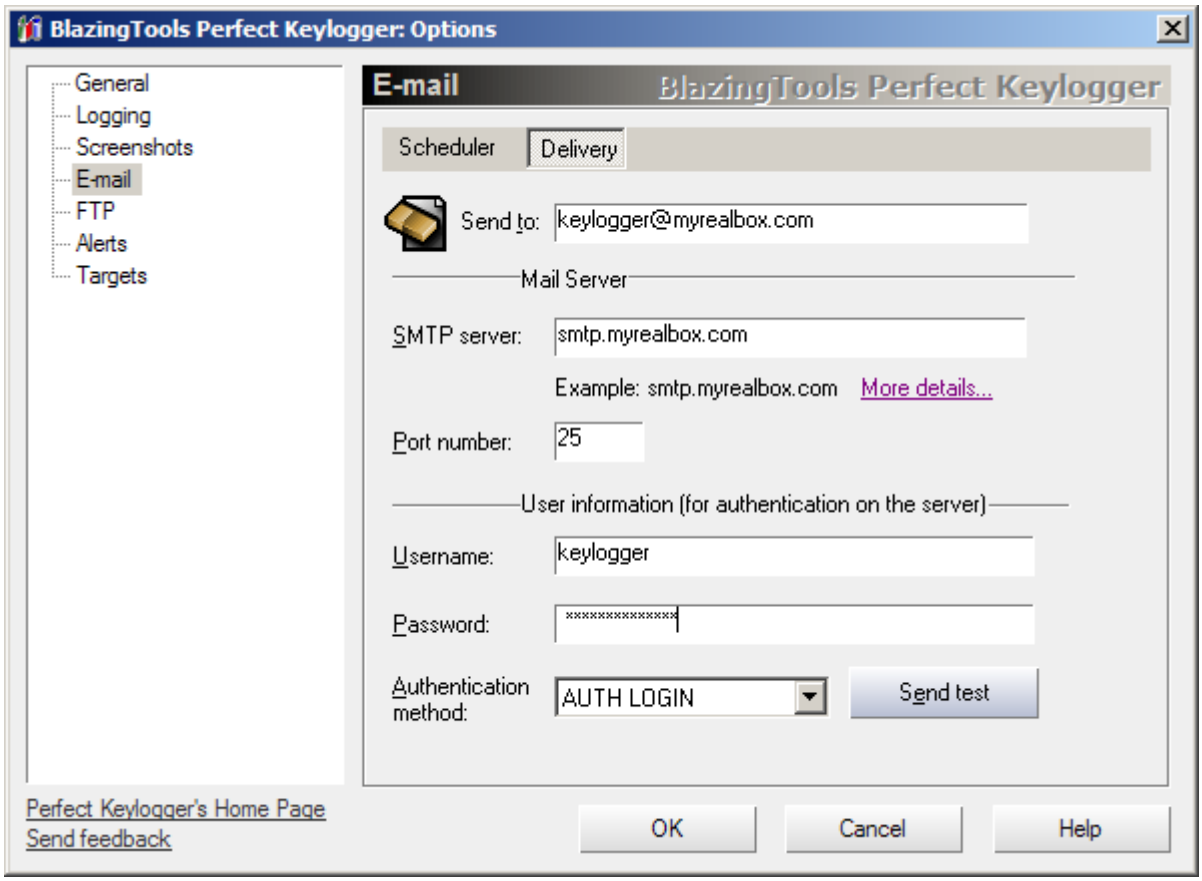
only when log size is more than _ kb

ส่วน option **Auto clean** จะทำให้ key logger เคลียร์ log ในเครื่อง remote เมื่อส่ง log ไปยังอีเมลเป้าหมายแล้ว



คลิกที่ปุ่ม **Delivery** ที่ **Send to** ให้ใส่ email address ที่จะส่ง log ไปให้ คุณสามารถใช้บริการฟรีได้จาก www.myrealbox.com ตามตัวอย่างข้างล่าง หรือดูรายชื่อผู้ให้บริการฟรีเพิ่มเติมจาก http://www.fepg.net/providers.html

คุณไม่สามารถใช้บริการของ Hotmail หรือ Yahoo ได้ เนื่องจากทั้งสองแห่งนี้ไม่ได้ใช้ SMTP server



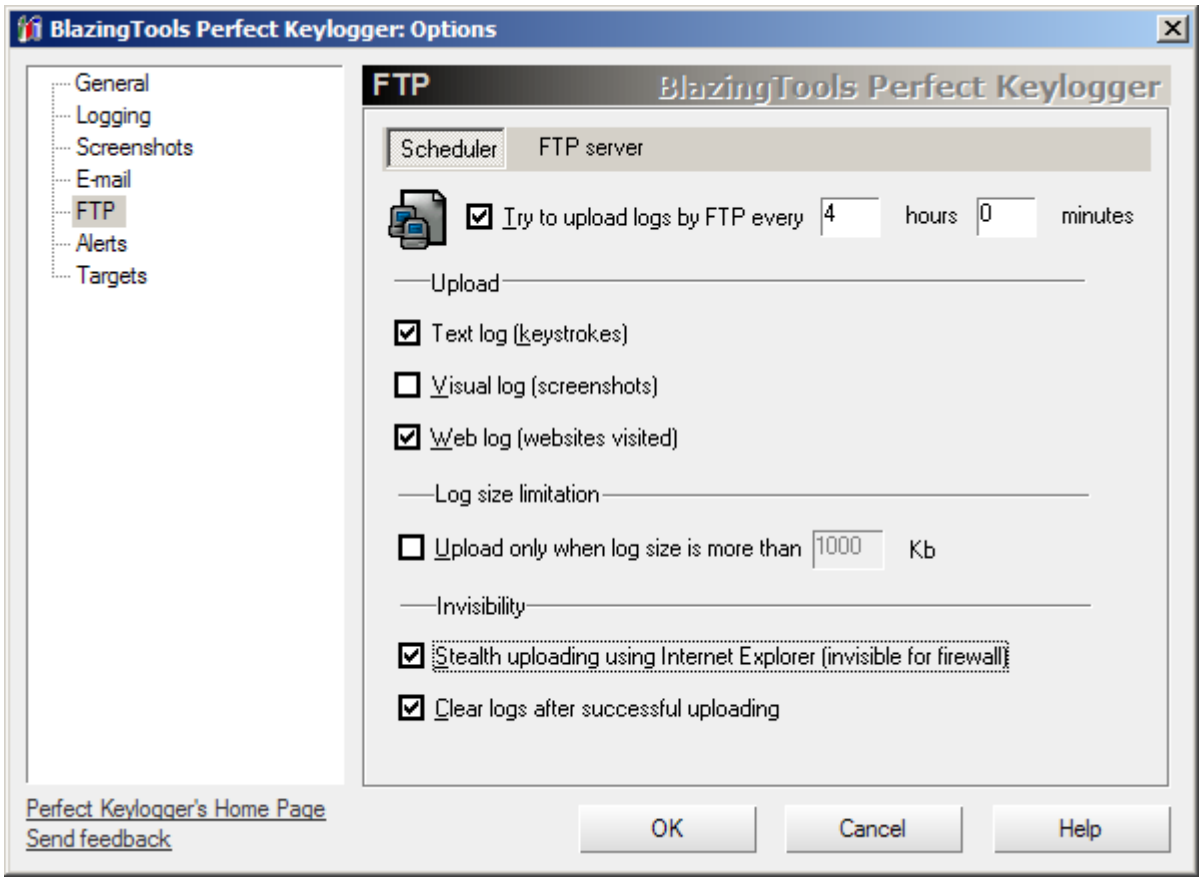
ในกรณีที่เครื่อง remote มีการติดตั้ง firewall การส่ง log ทางอีเมลจะไม่ได้ผล วิธีที่สามารถหลบหลีกการตรวจจับจาก firewall จึงต้องใช้วิธีการส่ง log ทาง ftp แทน (ต้องปิดการทำงานของ email ด้วย เพื่อไม่ให้สามารถถูกตรวจจับจาก firewall) โดยกำหนดให้ส่งทาง ftp ผ่านทางโปรแกรม Internet Explorer โดยเลือกที่ **Stealth uploading using Internet Explorere** (invisible for firewall) เนื่องจาก firewall ส่วนใหญ่จะให้ trust กับ Internet Explorer อยู่แล้ว

Global Technology Integrated Co.,Ltd.

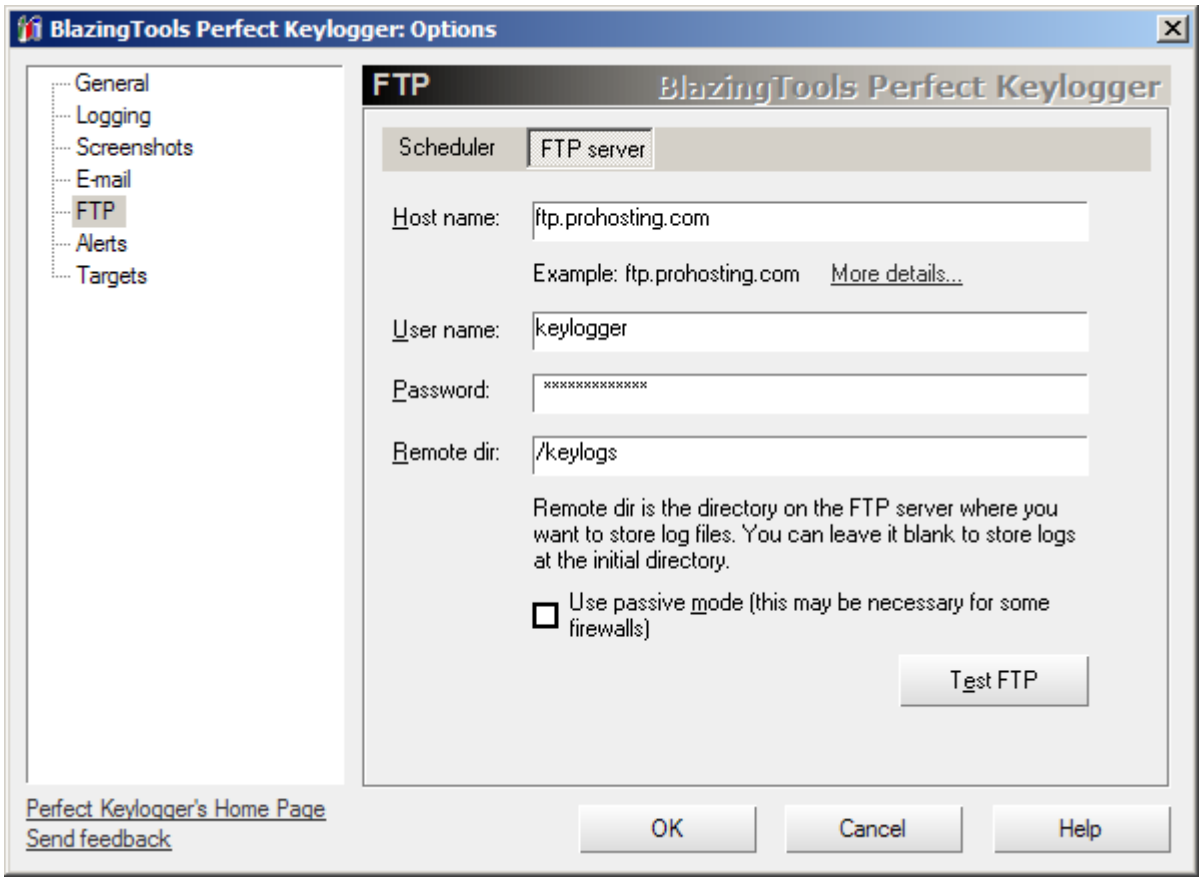
99/349 Moo 2, Chaengwattana Rd., Tungsonghong, Laksi, Bangkok 10210

Tel : 0 2982 3338-9 , Fax : 0 2982 3338-9 ext. 11

www.gbtech.co.th



ใส่ ftp server พร้อม User name, Password และไดเร็กทอรีที่ต้องการให้ upload log ลงไปด้วย ทั้งนี้ควรสมัครบริการ ftp server ที่ให้เนื้อที่ฟรีซึ่งสามารถดูได้จาก Google directory



เมื่อกำหนดค่าในเมนู option เสร็จเรียบร้อย ต่อมาจึงเริ่มการใช้งาน Remote installation โดยคลิกขวาเลือกที่เมนู แล้วคลิกที่ **Remote installation** ก่อนที่จะถึงขั้นตอนนี้ต้องแน่ใจว่า ได้เลือก option "**Run at Windows startup**", "**Don't show program icon at startup**" และได้กำหนดค่าสำหรับการส่ง log ทาง mail และ/หรือ FTP แล้ว

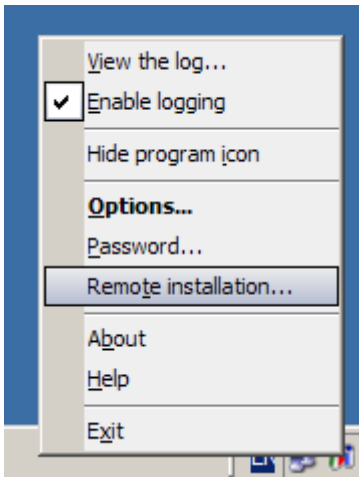
การส่ง keylogger ไปยังเครื่อง Remote (Remote Installation)

คลิกขวาที่ไอคอนของ keylogger แล้วเลือกที่ Remote installation

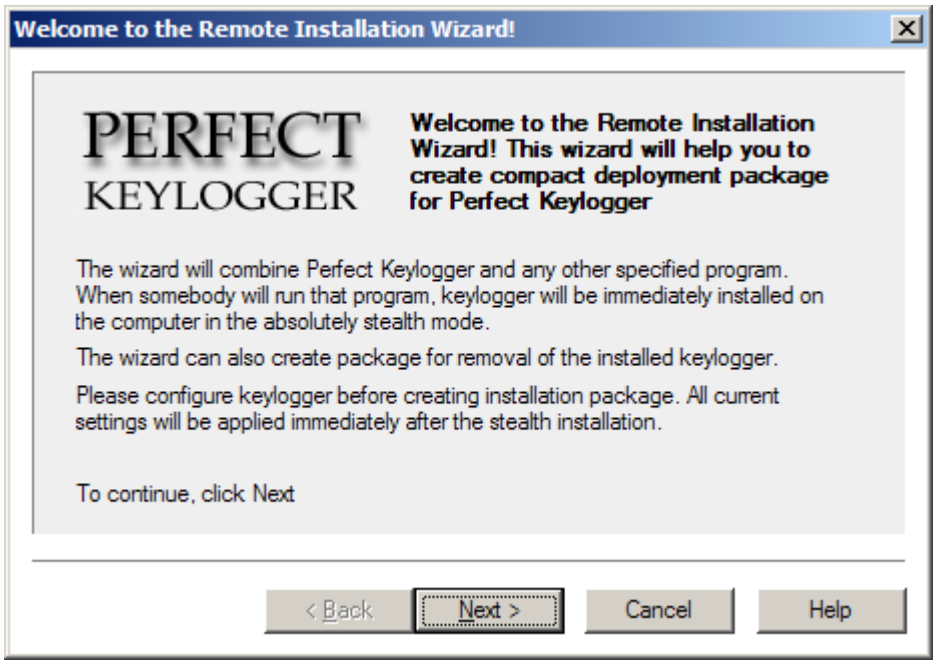
99/349 Moo 2, Chaengwattana Rd., Tungsonghong, Laksi, Bangkok 10210

Tel : 0 2982 3338-9 , Fax : 0 2982 3338-9 ext. 11

www.gbtech.co.th



จะปรากฏวินโดวส์ดังต่อไปนี้ แล้วคลิกที่ **next**



Global Technology Integrated Co.,Ltd.

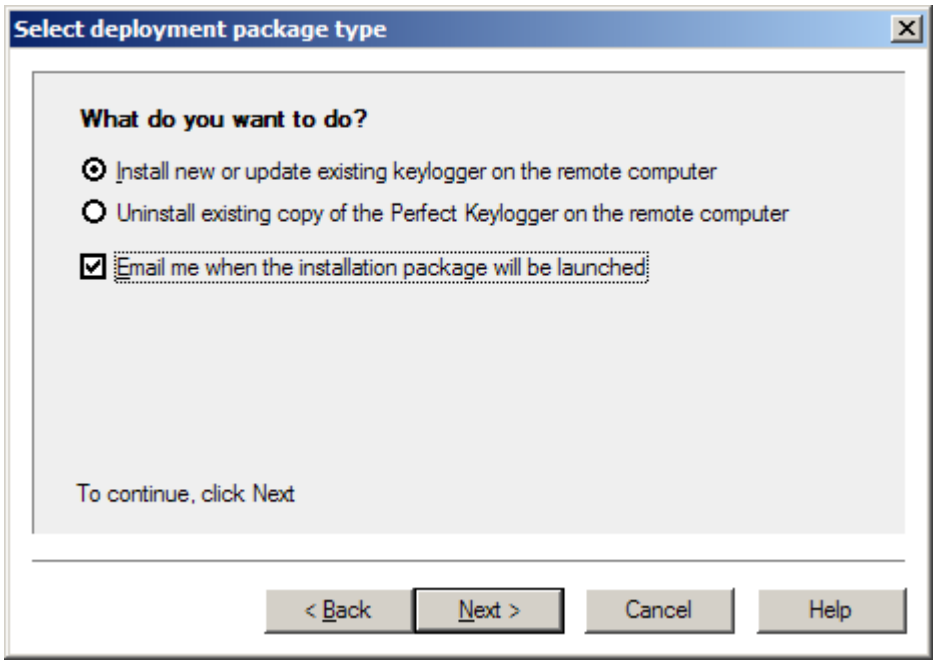
99/349 Moo 2, Chaengwattana Rd., Tungsonghong, Laksi, Bangkok 10210

Tel : 0 2982 3338-9 , Fax : 0 2982 3338-9 ext. 11

www.gbtech.co.th

เลือกที่ **Install new or update existing keylogger on the remote computer**

เมื่อโปรแกรมนั้นได้ถูกเปิดในเครื่องเป้าหมายแล้ว ถ้าต้องการให้โปรแกรมส่งอีเมลมาแจ้งให้เลือกที่ **Email me when the installation package will be launched** ด้วย

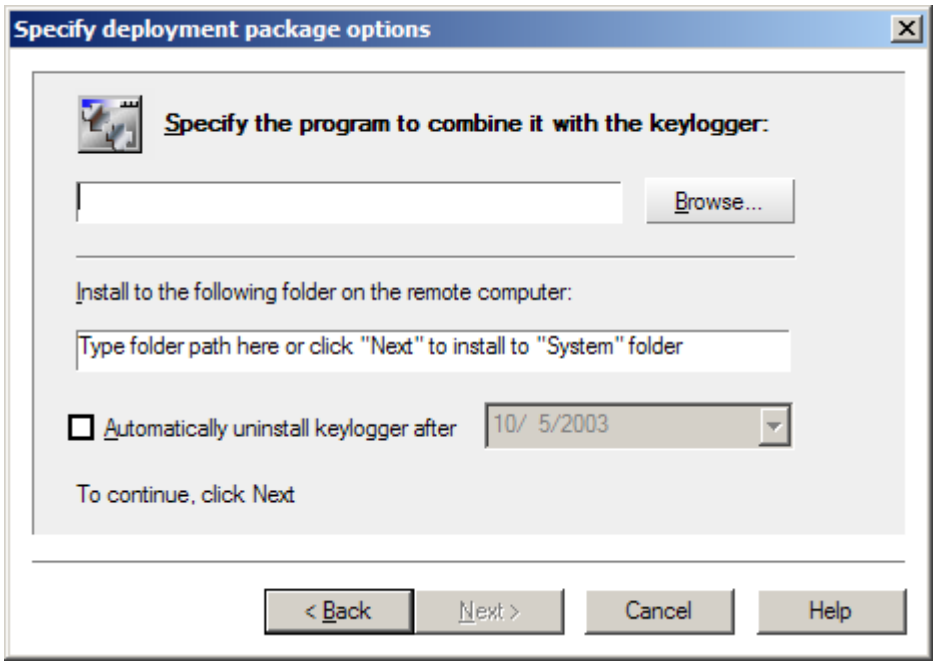


ต่อไปจึงเลือกโปรแกรม .exe ที่จะให้มี keylogger รวมไปอยู่ด้วย

99/349 Moo 2, Chaengwattana Rd., Tungsonghong, Laksi, Bangkok 10210

Tel : 0 2982 3338-9 , Fax : 0 2982 3338-9 ext. 11

www.gbtech.co.th



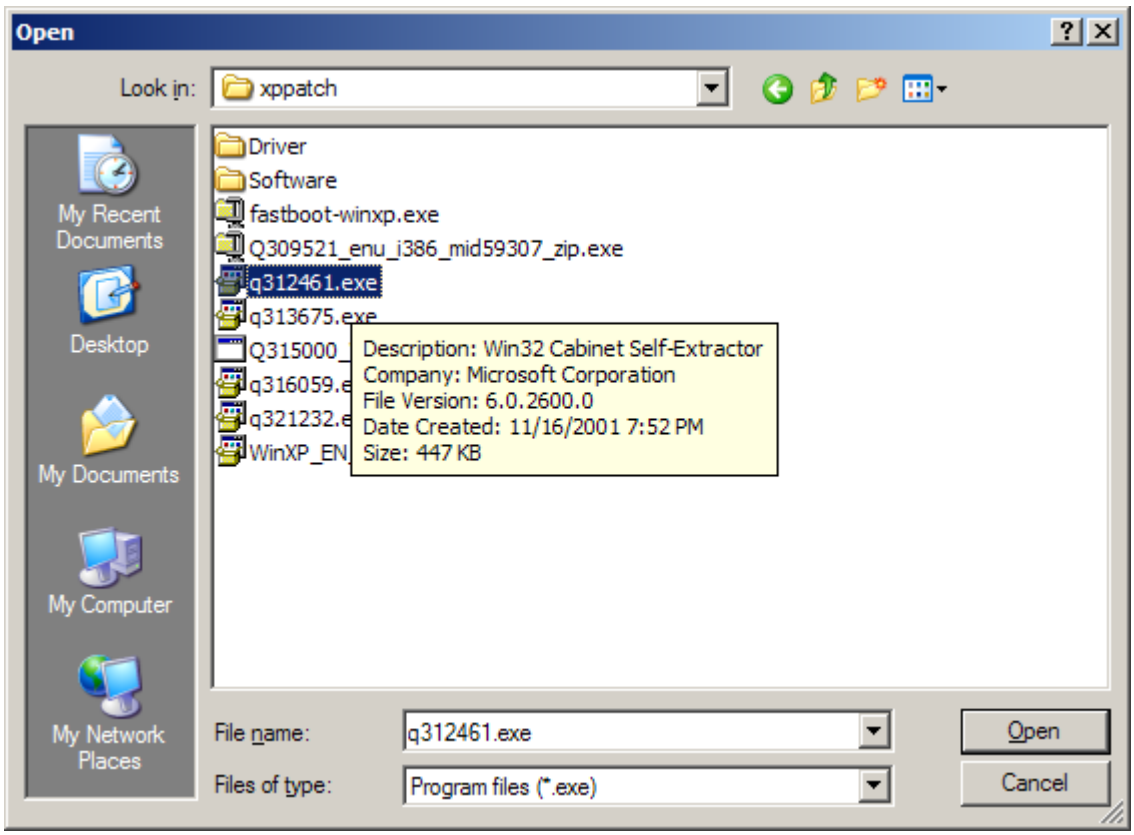
เลือกไฟล์ .exe ที่ต้องการให้ keylogger ฝังตัวเองอยู่ด้วย

Global Technology Integrated Co.,Ltd.

99/349 Moo 2, Chaengwattana Rd., Tungsonghong, Laksi, Bangkok 10210

Tel : 0 2982 3338-9 , Fax : 0 2982 3338-9 ext. 11

www.gbtech.co.th

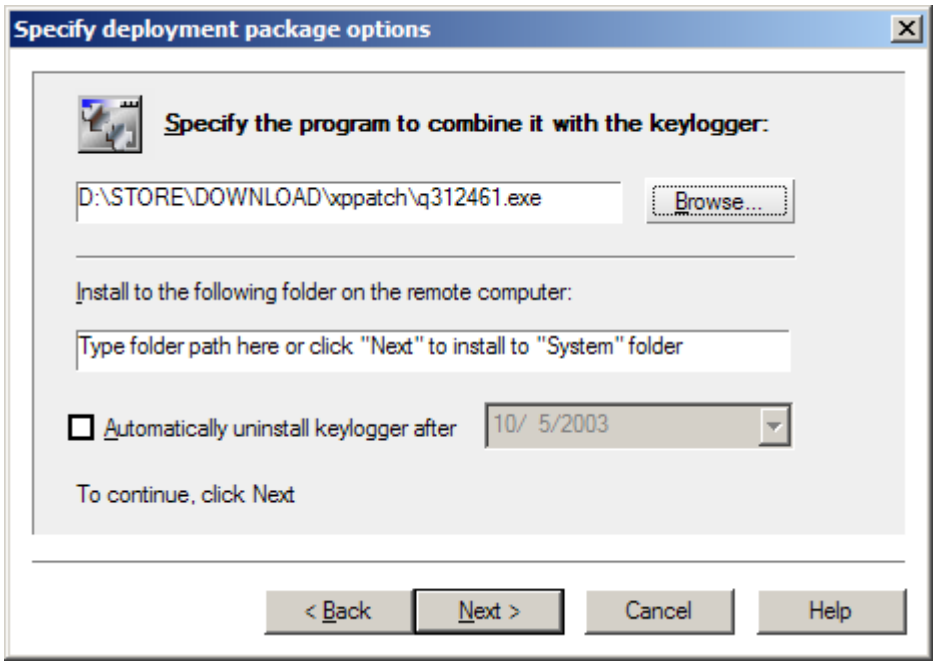


ถ้าต้องการให้ key logger ติดตั้งที่ folder อื่น แทนที่จะเป็น system folder (โดยค่า default จะเป็น "Windows\System" สำหรับ Windows 9.x/Me และ"Winnt\System32" สำหรับ Windows NT/2000/XP.)ให้ใส่เข้าไปในช่อง **Install to the following folder on the remote computer** นอกจากนี้เรายังสามารถกำหนดให้ key logger uninstall ตัวมันเองในหลังจากเวลาที่กำหนดไว้โดยเลือกที่ Automatically uninstall keylogger after ... จากนั้นจึงคลิกที่ Next

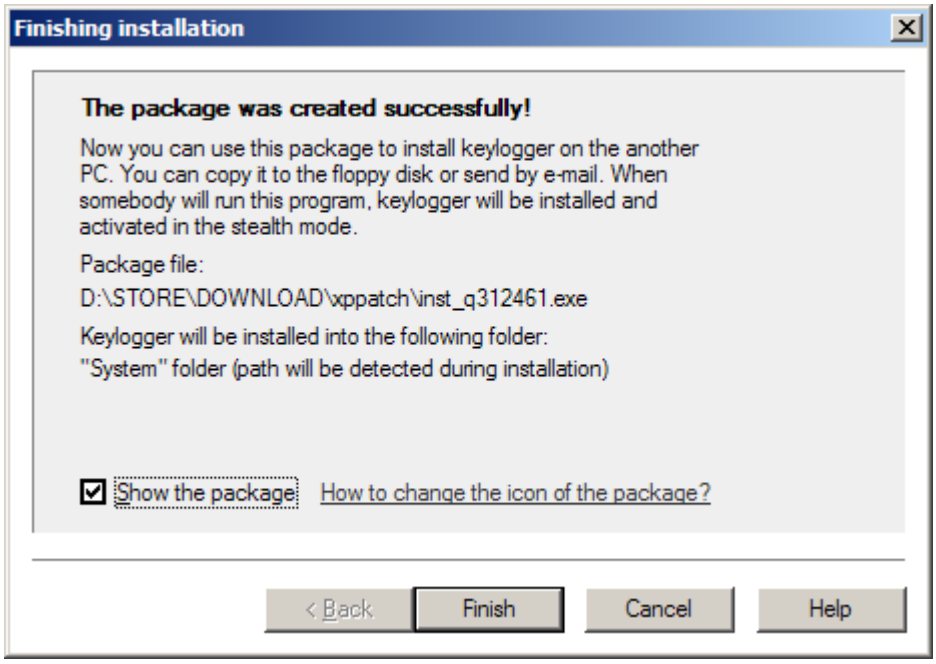
99/349 Moo 2, Chaengwattana Rd., Tungsonghong, Laksi, Bangkok 10210

Tel : 0 2982 3338-9 , Fax : 0 2982 3338-9 ext. 11

www.gbtech.co.th



จากนั้นจึงกดที่ Finish



Global Technology Integrated Co.,Ltd.

99/349 Moo 2, Chaengwattana Rd., Tungsonghong, Laksi, Bangkok 10210

Tel : 0 2982 3338-9 , Fax : 0 2982 3338-9 ext. 11

www.gbtech.co.th

จากนั้นจึงส่งไฟล์แนบไปกับอีเมล ส่งไปยัง email address ของเป้าหมาย แล้วใช้วิธีหลอกล่อแบบต่าง ๆ (social engineering) เพื่อให้เป้าหมายเปิดไฟล์ ที่แนบมาด้วย

เมื่อผู้ใช้เครื่องเป้าหมายเปิดไฟล์ที่แนบมา และได้ reboot เครื่องแล้ว keylogger จะเริ่มทำงาน และส่งอีเมลมายัง email address ที่เราต้องการดังรูป

kiattisak@gbtech.co.th Fri, 6:12 pm + Perfect Keylogger report: 3/10/2546, 18:12 (ACCOUN...
kiattisak@gbtech.co.th Fri, 6:06 pm + Perfect Keylogger report: 3/10/2546, 18:06 (ACCOUN...
kiattisak@gbtech.co.th Fri, 5:32 pm + Perfect Keylogger report: 3/10/2546, 17:32 (ACCOUN...

ตัวอย่างของอีเมลที่ส่งมา

Subject: Perfect Keylogger report: 3/10/2546, 18:12 (ACCOUNT\Administrator)
From: kiattisak@gbtech.co.th
Date: Fri, October 3, 2003 6:12 pm
To: kiattisak@gbtech.co.th
Priority: Normal
Options: View Full Header | View Printable Version | View Message details

```
This is a Perfect Keylogger report for computer "ACCOUNT", user "Administrator".

You can view attached log files directly with your e-mail program.
```

Attachments:

keystrokes.html	2.5 k	[application/octet-stream]	download | view
2003-10-03_18-07-29.jpg	106 k	[application/octet-stream]	download | view
2003-10-03_18-12-29.jpg	141 k	[application/octet-stream]	download | view

---

Global Technology Integrated Co.,Ltd.
99/349 Moo 2, Chaengwattana Rd., Tungsonghong, Laksi, Bangkok 10210
Tel : 0 2982 3338-9 , Fax : 0 2982 3338-9 ext. 11
www.gbtech.co.th

รอผลจาก e-mail ส่งมาเป็นระยะหลังจากเครื่องที่ติด trojan ได้ทำงานแล้ว

Global Technology Integrated Co.,Ltd.

99/349 Moo 2, Chaengwattana Rd., Tungsonghong, Laksi, Bangkok 10210

Tel : 0 2982 3338-9 , Fax : 0 2982 3338-9 ext. 11

www.gbtech.co.th