HACKING E-BOOK

FIRST EDITION

By Pound

หนังสือเชิงศึกษา ผู้เขียนจะไม่รับผิดชอบต่อการกระทำใดๆ ที่นำมาซึ่งความเสียหายแก่ผู้อื่น กรุณาใช้ในทางการศึกษาและใช้งานอยู่บนความรับผิดชอบของคุณเอง. ผมแนะนำให้อ่าน พ.ร.บ. คอมฯ ฉบับ ๒๕๕๐ ก่อนเริ่มศึกษานะครับ ทั้งนี้ก็เพื่อผลประโยชน์สูงสุดแก่ตัวผู้อ่านเอง และด้วยความปราถนาดีจากผู้เขียน - Pound

❖

To my parents, with love.

❖

Basic Hacking

DDoS Attack

Website Hacking

Pentesting

Safe Hacking

Protect Yourself

Facebook Hacking

แนะนำหนังสือ

สวัสดีครับสมาชิกที่รักทุกท่าน, หนังสือนี้เป็นหนังสือสอนแฮกสำหรับมือใหม่เล่มแรกของประเทศไทย มีทุกสิ่งรวมอยู่ในหนังสือเล่มนี้สำหรับมือใหม่ที่อยากเป็นแฮกเกอร์! หนังสือเล่มนี้เหมาะสำหรับมือใหม่ที่ไม่รู้จะเริ่มที่ไหนดี แต่คุณอาจจะเป็นหนึ่งในบุคคลจำพวกต่อไปนี้:

- ไม่มีประสบการณ์ด้านการแฮกเลย
- มีประสบการณ์บ้างเล็กน้อย
- มีประสบการณ์ความรู้เยอะพอสมควร

หนังสือเล่มนี้เหมาะสำหรับทุกคนครับ. ถึงคุณจะไม่ใช่มือใหม่ ผมค่อนข้างมั่นใจว่าคุณต้องได้ประโยชน์จากหนังสือเล่มนี้ไม่มากก็น้อย. หนังสือเล่มนี้จะรวบรวมบทความการสอนเกี่ยวกับการแฮกทุกรูปแบบตั้งแต่ *การสร้างโทรจัน Keylogger Stealer Phishing บอทเน็ต แฮกเว็ปไซต์ แฮกไวไฟ* เป็นต้น โดยใช้ภาษาบ้านๆ เข้าใจง่ายพร้อมรูปภาพประกอบเพื่อให้ง่ายต่อการปฏิบัติตาม สำหรับมือใหม่ที่ไม่มีประสบการณ์ หนังสือเล่มนี้จะเปลี่ยนคุณให้เป็นคนใหม่ในระยะเวลาอันสั้น.

ผมพยายามจะทำให้หนังสือเล่มนี้มีจำนวนหน้าน้อยที่สุด เพื่อลดความยุ่ง ซับซ้อนและยากต่อการทำความเข้าใจ. ดังนั้นบทความส่วนใหญ่ที่ถูกลงไว้ในบอร์ดอยู่แล้วผมจะไม่นำมาเขียนซ้ำในหนังสือเล่มนี้ แต่จะทำลิงค์เข้าไปในกระทู้ของบทความนั้นๆแทน นี้ก็เพื่อ:

- ลดจำนวนหน้าของหนังสือให้ได้มากที่สุด
- ลดความซับซ้อน
- ถ้าคุณไม่เข้าใจตรงไหนคุณสามารถโพสถามในกระทู้ได้ทันที
- ทำให้คุณเรียนรู้ได้เร็วขึ้น

หนังสือเล่มนี้จะช่วยให้คุณรู้ถึงหลักการในการแฮกทุกรูปแบบ รวมถึงเทคนิคและแนวทางต่างๆ *แต่..หนังสือเล่มนี้ไม่ได้สอนให้คุณแฮกเป็นอย่างเดียว แต่สอนให้คุณแฮกอย่างไรให้ปลอดภัยซึ่งเป็นสิ่งที่สำคัญที่สุดที่แฮกเกอร์หลายคนมองข้าม* นอกจากนี้คุณจะรู้วิธีการแฮกในรูปแบบต่างๆ และเทคนิคที่แฮกเกอร์ใช้ เพื่อนำไปเป็นแนวทางในการป้องการระบบเคลือข่ายของคุณให้ปลอดภัยจากแฮกเกอร์.

เริ่มกันที่โปรแกรม RAT

RAT มีสองประเภท:

- RAT ที่ย่อมาจาก Remote administrator tools - เป็นโปรแกรมถูกกฎหมายที่ใช้บังคับควบคุมคอมพิวเตอร์ของคนอื่นโดยการยินยอมจากทั้งสองฝ่าย เช่น Team Viewer
- RAT ที่ย่อมาจาก Remote access trojan - เป็นโปรแกรมที่ผิดกฎหมายที่ใช้สร้างตัวโทรจันเข้าไปควบคุมคอมพิวเตอร์ของคนอื่น เช่น Dark Comet, Cybergate, Spy Net และอื่นๆ

คุณสมบัติของ RAT:

- ควบคุมคอมพิวเตอร์ของเหยื่อ (ควบคุมเต็มรูปแบบโดยเหยื่อไม่รู้ตัว)
- ดาวน์โหลดข้อมูล ลบข้อมูล อัพโหลดข้อมูล
- Keylogger (ดักคีย์บอร์ด)
- Stealer (ขโมยรหัสผ่านต่างๆ)
- ดู Webcam ของเหยื่อ
- ดูหน้าจอ
- ใช้งาน cmd
- และอื่นๆอีกมากมาย

คุณสามารถใช้งานคอมฯของเหยื่อได้ดีกว่าเจ้าของเครื่องเองสะอีก.

ลองไปดูวิดีโอกันหน่อยว่ามันทำงานยังไง...

https://youtu.be/0G9LAPY7YTA

วิธีตั้งค่าและสร้างโทรจัน

วิธีสร้างโทรจันโดย DarkComet RAT:
http://www.hackdee.net/community/index.php?threads/mueaaihm-withueaichnganaelakhamsangtang2ain-darkcomet-rat.116/

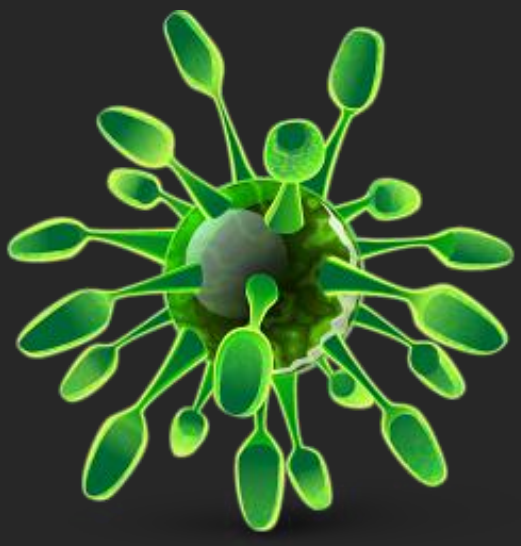
วิธีสร้างโทรจันโดย CyberGate RAT:
http://www.hackdee.net/community/index.php?threads/mueaaihm-withuetidtang-cybergate-rat-opraekrmsrangothrchan.3/

ผมแนะนำให้ใช้ **DarkComet RAT** นะครับเพราะว่า CyberGate ยังมีปัญหาเกี่ยวกับไฟล์ DLL. ที่เหลือก็ทำตามขั้นตอนให้ละเอียดนะครับ ถ้าเกิดเจอปัญหาวิธีแก้อยู่ในกระทู้นั้นหมดแล้ว แต่ถ้ายังทำไม่ได้ ให้ลองไล่อ่านคอมเม้นของสมาชิกท่านอื่นดู หรือโพสถามได้เลยครับ ทีมงานออนตลอด.

หลังจากที่ติดตั้งโปรแกรม RAT คุณอาจจะต้องเรียนรู้กับคำสั่งต่างๆ:

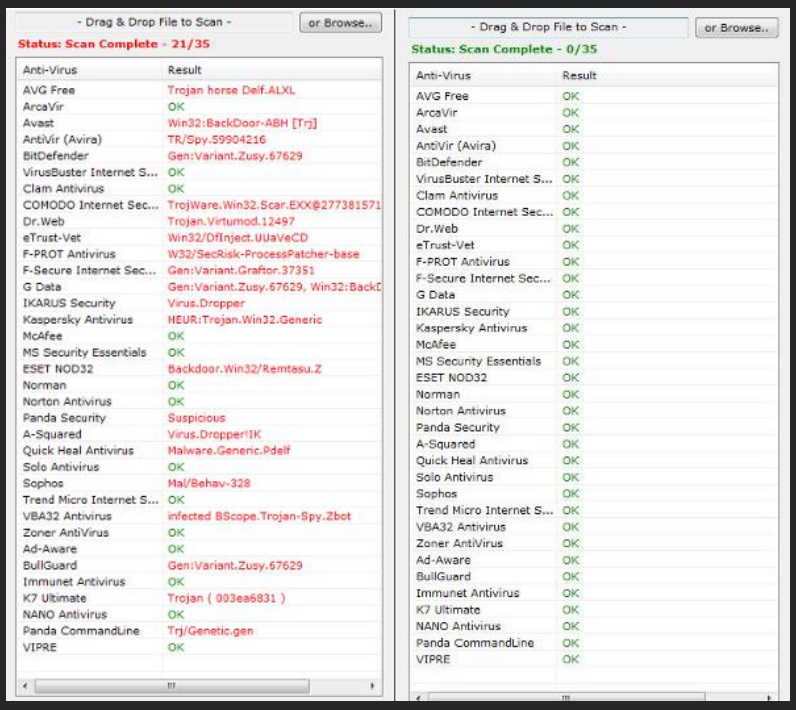
http://www.hackdee.net/community/index.php?threads/mueaaihm-withueaichnganaelakhamsangtang2ain-darkcomet-rat.116/

WARNING! ผมแนะนำให้คุณอ่านหัวข้อ **"แฮกปลอดภัย"** ก่อนที่จะเริ่มแฮกใคร



รู้จักกับโปรแกรม Crypter

ในเมื่อหนังสือเล่มนี้ เป็นหนังสือสำหรับมือใหม่ ผมจะไม่อธิบายลึกซึ่งเกี่ยวกับโปรแกรม Crypter นะครับ ถ้าใครอยากลงลึกเรื่องการทำ Crypter ติดตาม **Hackdee 2nd Edition** เร็วๆนี้ครับ. Crypter คือโปรแกรมที่จะทำไฟล์ไวรัสต่างๆในสแกนไม่พบโดยบริษัทแอนตี้ไวรัสทั้งหลายดูตัวอย่างผลสแกน ก่อนและหลังการทำ Crypting:



Tip: ห้ามสแกนไฟล์โทรจันของคุณลงบนเว็ปสแกนไวรัสอื่นนอกจาก 2 เว็ปนี้:
http://www.scan4you.net (เสียตัง)
http://www.nodistribute.com (ฟรี 4 ครั้งต่อวัน)

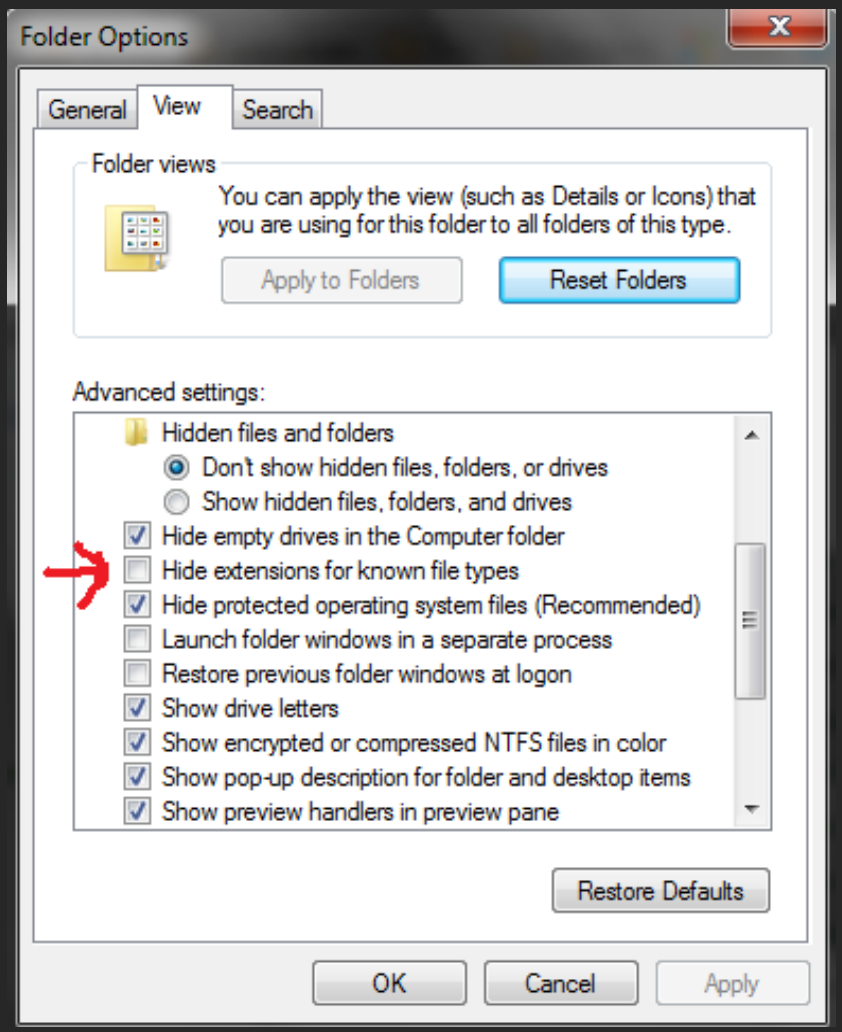
เพราะว่าเว็ปอื่นๆเช่น www.virustotal.com มันจะส่งผลสแกนไปให้บริษัทแอนตี้ไวรัสต่างๆโดยอัตโนมัติ ทำให้โทรจันของเราถูกสแกนเจอได้เร็วขึ้น.

วิธีเปลี่ยนนามสกุลไฟล์

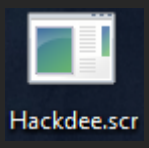
หัวข้อนี้จะสอนวิธีเปลี่ยนนามสกุลไฟล์ Executable (.exe .com .bat .cmd .scr) เป็นนามสกุลอะไรก็ได้ที่ดูน่าเชื่อถือเช่น .png .jpg .mp3 ฯลฯ....

Tip: ผมแนะนำให้สร้างโทรจันโดยใช้นามสกุล .scr นะครับเพราะมันดูน่าเชื่อถือมากกว่านามสกุลอื่นๆ เช่น .exe .com .bat..

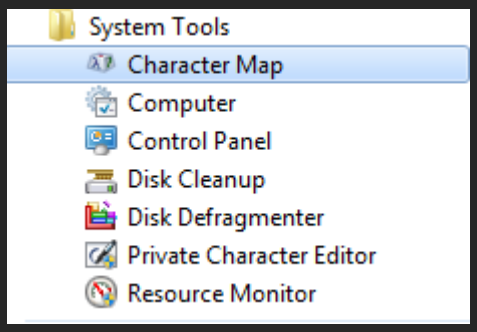
ก่อนอื่นเลยข้อนี้สำคัญมากห้ามข้ามเด็ดขาด!!... ไปที่ **Start > Control Panel > Folder Options** ในช่อง **View** เลื่อนลงมาหาบรรทัดที่ชื่อว่า **"Hide extensions for known file types"** ติกมันออกไป (ปล่อยว่างไว้) จากนั้นกด **Apply** แล้วก็ **OK**:



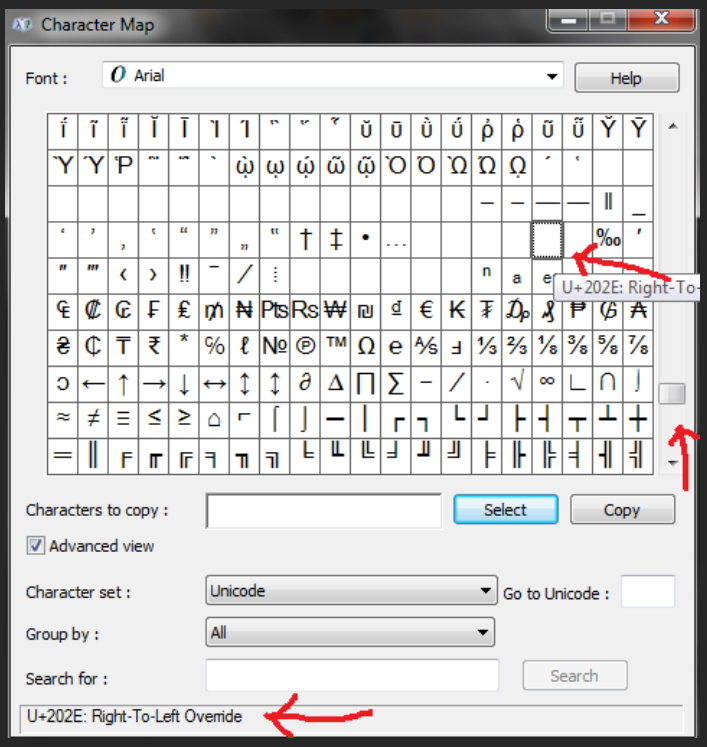
จะทำให้เราเห็นนามสกุลไฟล์ของไฟล์ทุกไฟล์:



จากนั้นไปที่ **Start > All Programs > Accessories > System Tools > Character Map:**



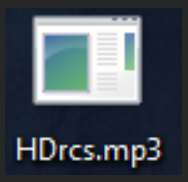
เลื่อนลงมาเรื่อยๆจนกว่าจะเจอตัวอักษรที่ชื่อว่า **"U+202E: Right-To-Left Override"** มันจะเป็นช่องว่างๆค่อยๆเลื่อนลงมาหา ตามรูป:



จากนั้นคลิก **"Select"** แล้วตามด้วย **"Copy"** (ไม่ต้องพิมพ์อะไรลงไปในช่อง Characters to copy นะครับ).

ไปที่ไฟล์ของคุณแล้วคลิกขวาเพื่อเปลี่ยนชื่อ **ชื่อไฟล์ของคุณต้องไม่ยาวเกินไปนะครับไม่งั้นมันจะเด้งกลับไปที่เก่า** (2-3 ตัวกำลังดี) จากนั้นนำเมาส์

ไปวางข้างหน้า "**.scr**" แล้วคลิกขวา > "**Paste**" พอถึงตรงนี้นามสกุลไฟล์ของคุณก็จะกลับหัวเป็น "**rcs.**" จากนั้นพิมพ์ชื่อนามสกุลไฟล์ที่คุณต้องการจะเปลี่ยน (พิมพ์กลับหัวนะครับ เช่นถ้าจะเปลี่ยนเป็น mp3 ก็ให้พิมพ์ 3pm) ถ้าทุกอย่างโอเคไฟล์ของคุณจะออกมาเป็นแบบนี้:



ถ้าเครื่องของคุณไม่มี Character Map ให้โหลดโปรแกรม "**BabelMap**" มาใช้แทนได้นะครับ ตามลิงค์นี้เลย:
http://www.babelstone.co.uk/Software/BabelMap.html

หรือถ้าขี้เกียจทำเองคุณสามารถใช้โปรแกรม **Hackdee's Spoofer** ได้:
http://www.hackdee.net/community/index.php?threads/hackdee-spoofer-opraekrmeplueynnamskulaifl.113/

วิธีรวมไฟล์

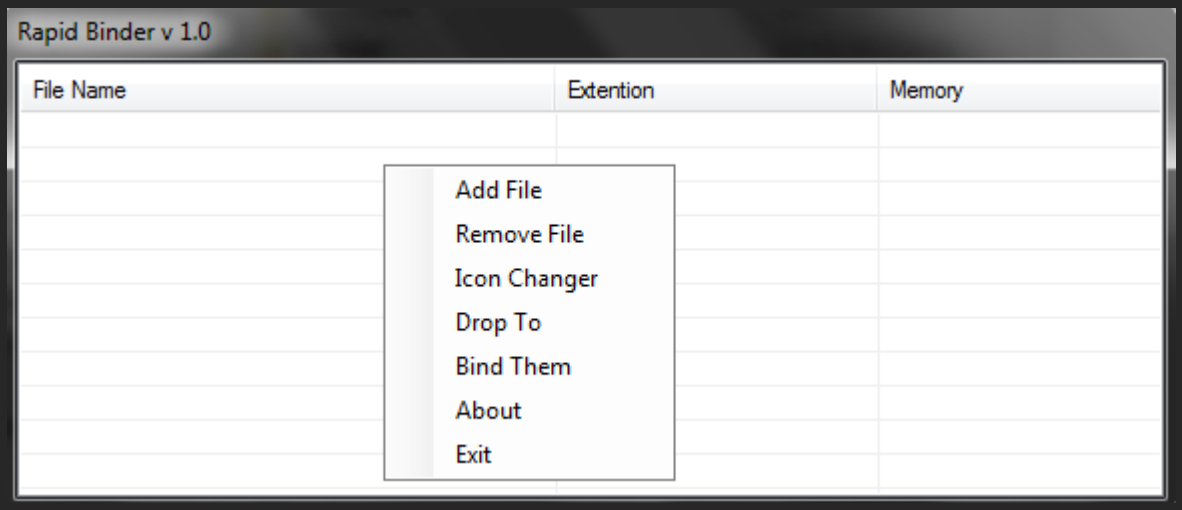
เราสามารถรวมไฟล์สองไฟล์ (หรือมากกว่า) เข้าด้วยกัน เช่นถ้าเราเอาไฟล์โทรจันไปรวมกับไฟล์เพลง พอเหยื่อกดเปิดไฟล์เรา ทั้งเพลง ทั้งโทรจัน ก็จะทำงานทั้งสองไฟล์...

ถ้าคุณใช้โปรแกรม DarkComet RAT มันจะมีตัวเลือกให้คุณทำการรวมไฟล์ระหว่างที่คุณกำลังสร้างโทรจันในหน้า File Binder.

แต่ถ้าคุณใช้ RAT ตัวอื่นที่ไม่มีตัวเลือกให้ทำการรวมไฟล์ เราจำเป็นต้องใช้อุปกรณ์ช่วย คุณสามารถหาโหลดได้ตาม www.Google.com ค้นหาคำว่า File Binder หรือ Exe Binder แต่ระวังหน่อยนะครับเพราะอาจมีของแถมฝังติดมาด้วย แต่ถ้าไม่อยากเสี่ยง ให้ใช้ของพื้นฐานตัวนี้ก็ได้ครับ:

https://www.mediafire.com/?606tfxr0bzrjkaq

วิธีใช้ก็ไม่ยากครับ นำไฟล์ที่เราจะรวมเข้าด้วยกันมาไว้ในโฟลเดอร์เดียวกัน จากนั้นเปิดโปรแกรม Rapid Binder ขึ้นมาแล้วกดคลิกขวาบนหน้าโปรแกรม:



Add File = แอดไฟล์ที่เราจะนำมารวมกัน
Remove File = ลบไฟล์
Icon Changer = เปลี่ยนไอคอน
Bind Them = รวมไฟล์เข้าด้วยกัน

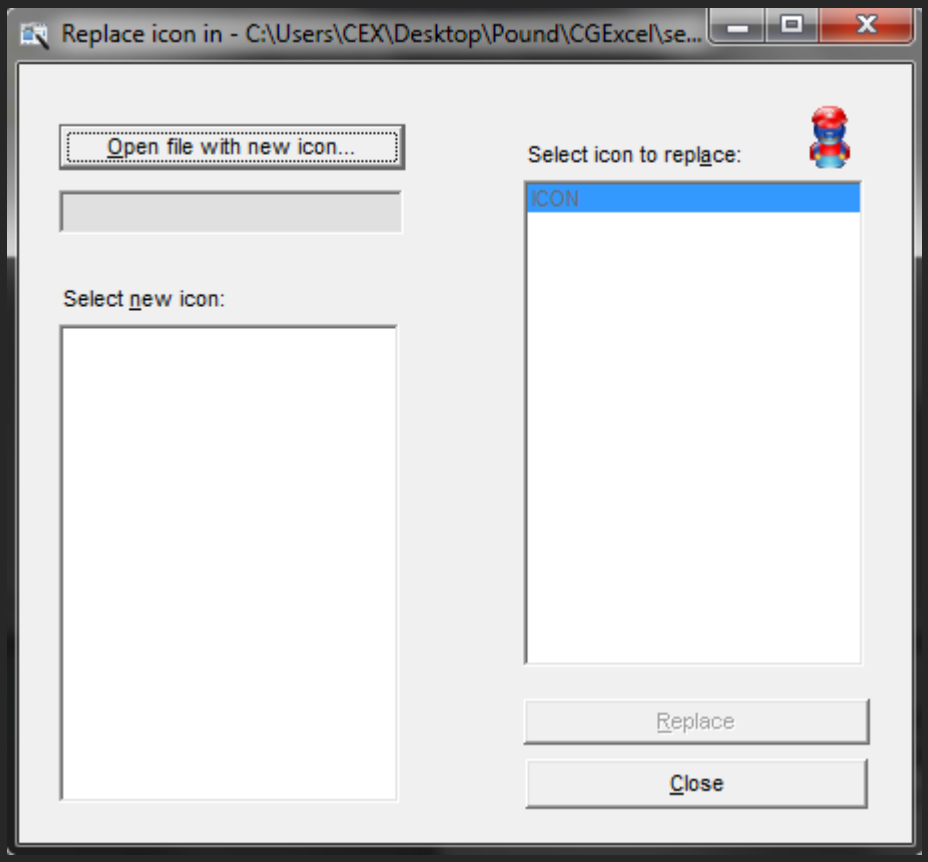
เปลี่ยนไอคอน

หัวข้อนี้เราจะใช้โปรแกรมที่ชื่อว่า **Resource Hacker** เข้ามาช่วย สามารถดาวน์โหลดได้จากลิงค์นี้เลย: http://www.angusj.com/resourcehacker

RAT ส่วนใหญ่มาพร้อมกับตัวเลือกให้เปลี่ยนไอคอนได้ ตอนเราสร้างโทรจัน แต่ถ้าคุณมีเหตุผลที่ต้องการเปลี่ยนไอคอนทีหลังหรือ RAT ที่คุณใช้ไม่มีตัวเลือกให้เปลี่ยนไอคอน ให้ทำตามวิธีต่อไปนี้:

เปลี่ยนไอคอน (สำหรับไฟล์ที่มีไอคอนอยู่แล้ว)

เปิดโปรแกรม **Resource Hacker** ขึ้นมา ไปที่ **File** > **Open..** แล้วเปิดไฟล์ที่คุณต้องการเปลี่ยนไอคอนขึ้นมา จากนั้นไปที่ **Action** > **Replace Icon ...** แล้วกดปุ่ม **Open file with new icon..** เพื่อเลือกไอคอนใหม่ที่เราจะเปลี่ยน:

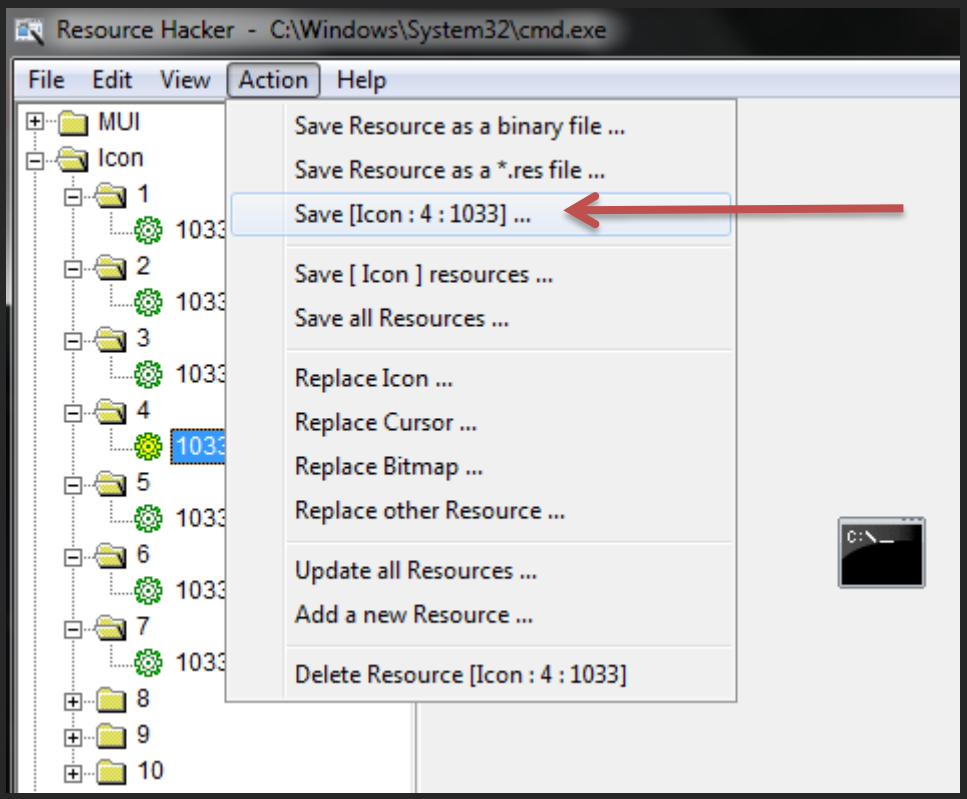


ใส่ไอคอน (สำหรับไฟล์ที่ยังไม่มีไอคอน)

เปิดโปรแกรม **Resource Hacker** ขึ้นมา ไปที่ **File** > **Open..** แล้วเปิดไฟล์ที่คุณต้องการเปลี่ยนไอคอนขึ้นมา จากนั้นไปที่ **Action** > **Add a new resource ...** คลิกปุ่ม **Open file with new resource..** เพื่อเลือกไอคอน จากนั้นในช่อง "Resource Name:" ตั้งชื่ออะไรก็ได้ แล้วกด Add Resource.

Copy ไอคอน

ในกรณีที่คุณต้องการใช้ไอคอนของโปรแกรมๆหนึ่งแต่คุณหาใน Google เท่าไหร่ก็หาไม่เจอ หรือเจอแต่ไม่เหมือนของจริงสักที.. ง่ายๆครับเปิด **Resource Hacker** ขึ้นมาแล้วเปิดโปรแกรมที่มีไอคอนที่คุณต้องการจะใช้ ในช่อง "**Icon**" คุณจะเห็นไอคอนหลายตัวให้เลือกอันที่ใกล้เคียงที่สุดแล้วไปที่ "**Action**" แล้ว "**Save [Icon] ...**" ตามรูปด้านล่าง:



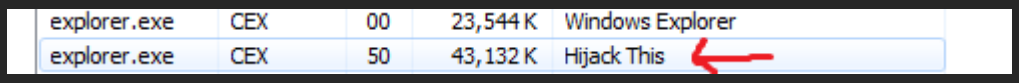
Tip: วิธีเปลี่ยนรูป jpg, png, gif ให้เป็น .icon:
http://converticon.com/

เปลี่ยนแปลงข้อมูลของไฟล์

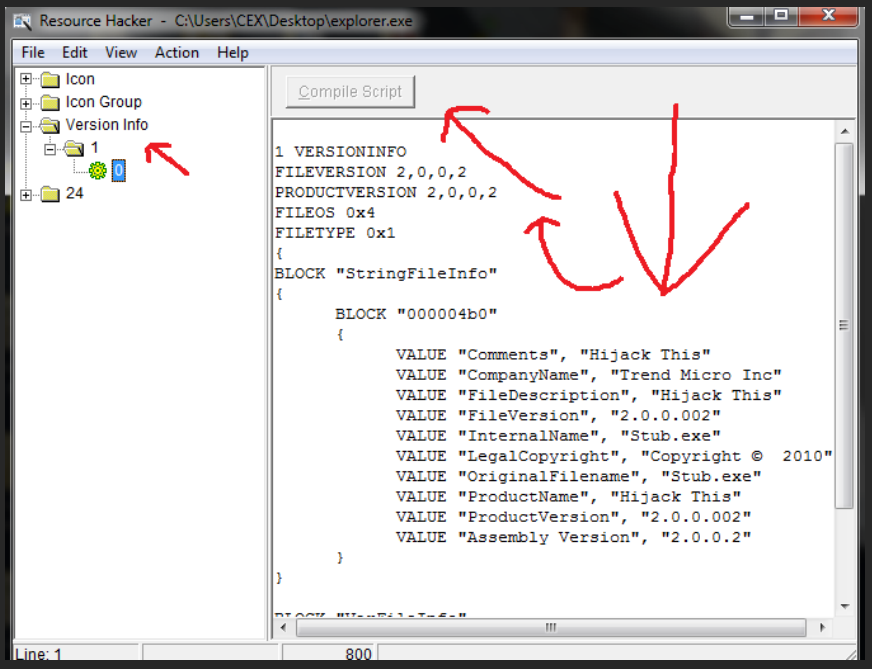
เปลี่ยนแปลงข้อมูลของไฟล์ (สำหรับไฟล์ที่มีข้อมูลอยู่แล้ว)
อีกหนึ่งวิธีที่คุณสามารถเพิ่มความน่าเชื่อถือให้กับไฟล์ของคุณคือการเปลี่ยนข้อมูลแหล่งที่มาของไฟล์ให้ดูน่าเชื่อถือ ยกตัวอย่างเช่นไฟล์โทรจันไฟล์นี้:

(ไฟล์โทรที่รวมเข้ากับไฟล์อื่นและเปลี่ยนไอคอนโดยใช้โปรแกรม Rapid Binder)

ข้อมูลแหล่งที่มาของไฟล์ข้างต้นดูไม่น่าเชื่อถือนัก ถึงแม้ว่าคุณจะเปลี่ยนชื่อไฟล์เป็น explorer.exe มันก็ยังโชว์ใน **Task manager** > **Processes** ของเหยื่อว่า "**Hijack This**" อยู่ดี เช่น:



เปิด Resource Hacker ขึ้นมาแล้วเปิดไฟล์ที่ขึ้นต้องการจะเปลี่ยนข้อมูล จากนั้นให้ไปที่ Version Info:



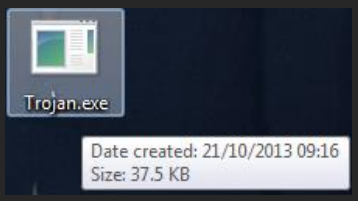
เปลี่ยนข้อมูลของไฟล์ตามนี้คุณต้องการ (ช่อง File Description คือช่องที่จะแสดงใน Processes นะครับ เปลี่ยนให้ดูน่าเชื่อถือหน่อย) จากนั้นคลิกที่ปุ่ม "**Compile Script**" ด้านบนแล้ว "**File** > **Save**" แค่นี้คุณก็จะได้ไฟล์โทรจันที่มีแหล่งข้อมูลที่น่าเชื่อถือแล้ว ^^.

Tip 1: ช่องไหนคุณไม่ต้องการ ให้ลบแค่ชื่อออกนะครับไม่ต้องลบทั้งบรรทัด เดียวมันจะเออเร่อ เช่น บรรทัด VALUE "**CompanyName**" , "**Trend Micro Inc**" ถ้าคุณไม่ต้องการคุณก็ลบแค่คำว่า Trend Micro Inc ซึ่งจะได้แบบนี้ VALUE "**CompanyName**" , ""

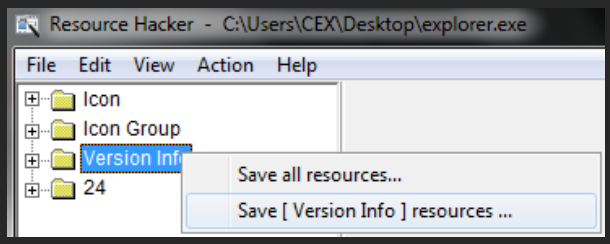
Tip 2: เปลี่ยนข้อมูลแหล่งที่มาของไฟล์ให้เข้ากับชื่อไฟล์ที่คุณจะตั้ง!

เพิ่มข้อมูลของไฟล์ (สำหรับไฟล์ที่ยังไม่มีข้อมูล)

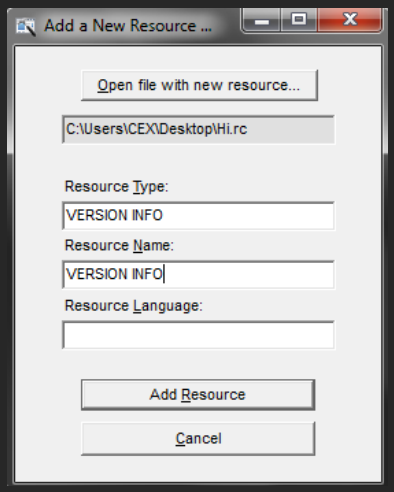
ไฟล์โทรจันที่สร้างโดย RAT ส่วนใหญ่จะไม่มีข้อมูลที่มาของไฟล์มาให้แต่แรก ซึ่งมันไม่น่าเชื่อถือเท่าไหร่นัก:



วิธีเพิ่มข้อมูลแหล่งที่มาก็ไม่ยากครับ ให้เปิด Resource Hacker ขึ้นมาแล้วเปิดไฟล์อะไรก็ได้ที่มีข้อมูลแหล่งที่มาอยู่แล้วขึ้นมา จากนั้นคลิกขวาที่ "**Version Info**" แล้วคลิกที่ "**Save [Version Info] Resource ...**" Save ไว้หน้า Desktop ของคุณจะได้ง่ายต่อการหา.



จากนั้นเปิดไฟล์โทรจันที่เราต้องการจะเพิ่มข้อมูลแหล่งที่มาลงไป แล้วไปที่ "**Action > Add a new Resource ...**" แล้วก็เลือกไฟล์ Resource ที่เรา Save ไว้ตอนแรก:



ช่อง "**Resource Type:**" และ "**Resource Name:**" ตั้งชื่อว่า Version Info จากนั้นกด "**Add Resource**" แล้วก็แก้ไขข้อมูลแหล่งที่มาตามใจคุณ.

สาธิตการสร้างโทรจันแบบเนียนๆ

หัวข้อที่ผ่านๆมาเราได้เรียนเกี่ยวกับวิธีสร้างโทรจัน การรวมไฟล์ เปลี่ยนนามสกุล การเปลี่ยนไอคอน และการเปลี่ยนข้อมูลแหล่งที่มาของไฟล์. หลายท่านอาจคิดว่าถ้าหากทำทั้งหมดเลยคงใช้เวลานาน.. ไม่เลยครับ ถ้าฝึกบ่อยๆ คุณสามารถสร้างโทรจันที่น่าเชื่อถือได้ภายในเวลาแค่ **2 นาที!** ผมจะสรุปวิธีสร้างโทรจันแบบเนียนๆให้ดูในหัวข้อนี้

ผมแนะนำให้เรียงลำดับขั้นตอนดังนี้ครับ สร้างโทรจัน > รวมไฟล์ > เปลี่ยนนามสกุลไฟล์ > เปลี่ยนแปลงข้อมูล/ไอคอนของไฟล์:

สร้างโทรจัน

ถ้าหากคุณใช้ DarkComet RAT มันจะมีตัวเลือกให้คุณรวมไฟล์ และเปลี่ยนไอคอนได้เลยตอนสร้างโทรจันซึ่งจะทำให้ประหยัดเวลาไปได้อีกขั้น.

รวมไฟล์

ถ้าหาก RAT ของคุณไม่มีตัวเลือกให้รวมไฟล์ในขั้นตอนการสร้างโทรจัน ให้ทำมันโดยใช้โปรแกรม Binder ตามบทความที่ผ่านมาครับ. ให้ทำมันในขั้นตอนที่สองต่อจากการสร้างโทรจัน.

เปลี่ยนนามสกุลไฟล์

ตามด้วยขั้นตอนที่สาม เปลี่ยนนามสกุลไฟล์ตามที่คุณต้องการ โดยใช้ Character Map ที่สอนไปข้างต้น.

เปลี่ยนแปลงข้อมูลแหล่งที่มา และไอคอนของไฟล์

ขั้นตอนนี้อยู่ในขั้นตอนสุดท้ายเพราะว่าถ้าคุณทำการรวมไฟล์ และเปลี่ยนชื่อและนามสกุลไฟล์ตามที่คุณต้องการแล้ว คุณถึงสามารถเปลี่ยนไอคอนและแหล่งข้อมูลที่มาของไฟล์ให้เข้ากับไฟล์ที่คุณเอาไปรวมหรือนามสกุลของไฟล์ที่คุณเปลี่ยนได้.

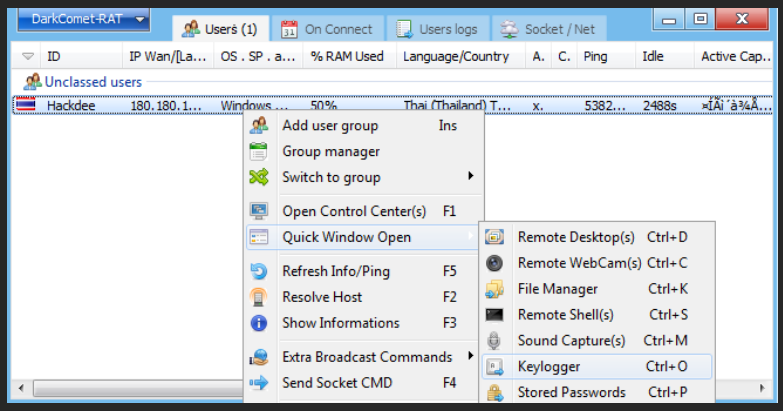
แค่นี้คุณก็จะได้ไฟล์โทรจันที่เนียนสุดๆ ^^

Keylogger และวิธีติดตั้ง

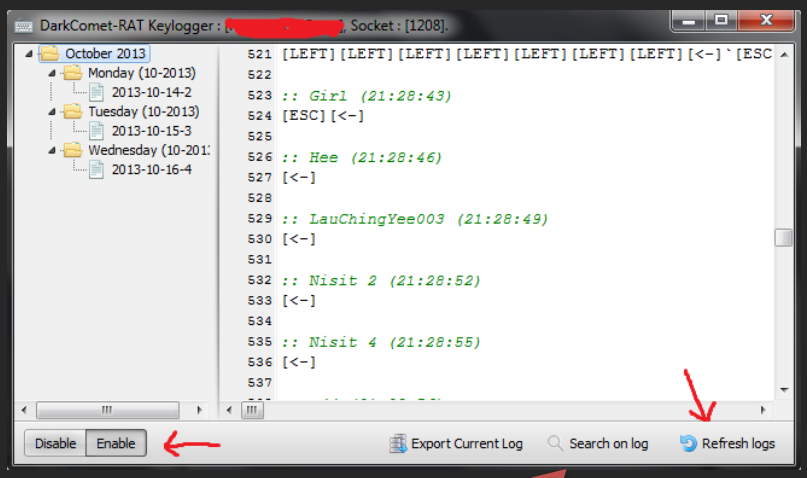
คีย์ล็อกเกอร์คือโปรแกรมที่สามารถดักการพิมพ์ หมายถึงถ้าเราพิมพ์อะไรโดยใช้คีย์บอร์ด มันก็จะถูกบันทึกไว้ทั้งหมด. คีย์ล็อกเกอร์จะแบ่งออกเป็น 2 ประเภท คือ แบบ Live Keylogging และ Logs Keyloggings

Live Keylogging

Live Keylogging คือฟังค์ชั่นที่เราสามารถ ดักและดู บันทึกการพิมพ์ของเหยื่อได้สดๆตอนนั้นเลย ฟังค์ชั่นประเภทนี้ส่วนใหญ่จะมากับโปรแกรม RAT ผมจะยกตัวอย่างคีย์ล็อกเกอร์ใน DarkComet RAT นะครับ. ให้เราคลิกขวาที่ชื่อบอท แล้วไปที่ "Quick Window Open" แล้วคลิกที่ Keylogger:



ในหน้า Keylogger ให้คลิก **Enable** แล้วกด **Refresh log** สักพักนึงบันทึกการพิมพ์ต่างๆก็จะแสดงอยู่บนหน้าจอ:



TIP: ถ้าล็อกมันเยอะไปให้ใช้ "Search on log" หาคีย์เวิร์ดที่เราต้องการนะครับ

Logs Keylogger

Logs Keylogger คือการส่งบันทึกการดักคีย์ไปเก็บไว้ในที่ๆหนึ่ง ซึ่งคุณสามารถมาเปิดดูตอนไหนก็ได้. การดักคีย์แบบนี้จะมีสองประเภท 1. ส่งบันทึกไปทางอีเมล 2. ส่งบันทึกผ่านทาง FTP เข้าไปเก็บไว้ในโฮสของเรา ประเภทที่สองคุณจำเป็นต้องมีโฮสนะครับ.

ส่งบันทึกไปทางอีเมล

ตัวเลือกนี้จะไม่มีใน RAT ครับ ส่วนใหญ่จะมีอยู่ในโปรแกรม Keylogger ทั่วไป สามารถหาโหลดได้ตาม www.Google.com นะครับแต่ผมไม่แนะนำให้โหลดจาก Google เลยเพราะมันไม่ปลอดภัย หรือใช้โปรแกรมที่แอดมินโพสไว้ในบอร์ดก็ได้พร้อมวิธีติดตั้ง ตามลิงค์ด้านล่าง:

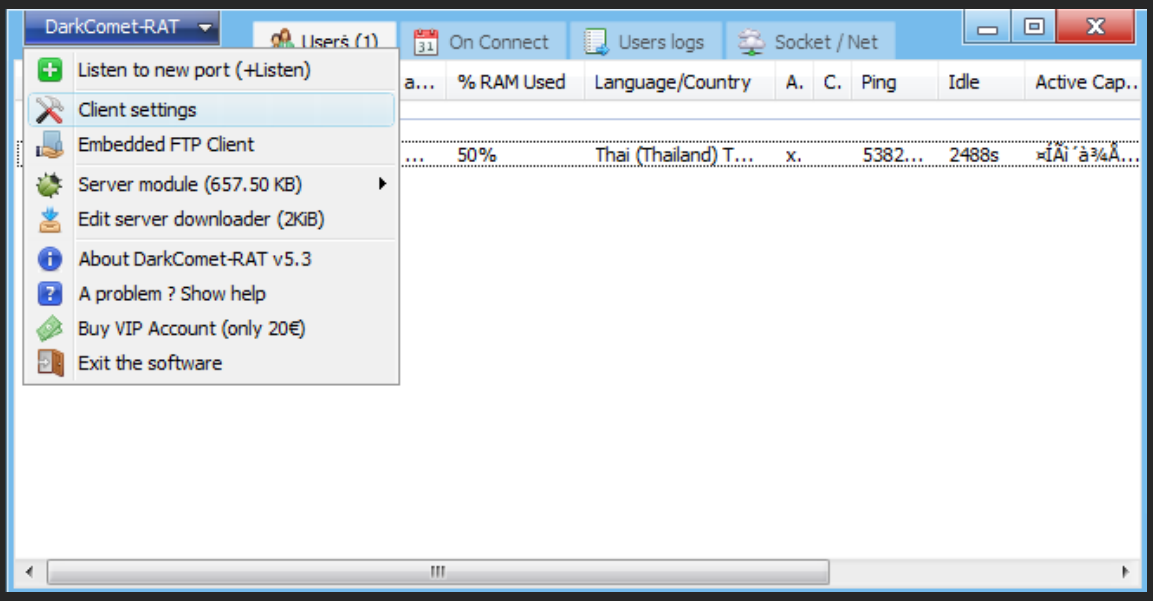
http://www.hackdee.net/community/index.php?threads/project-neptune-keylogger-phromwithuetidtang.1088/ Project Neptune Keylogger

http://www.hackdee.net/community/index.php?threads/withuetidtang-keylogger.94/ Syslogger

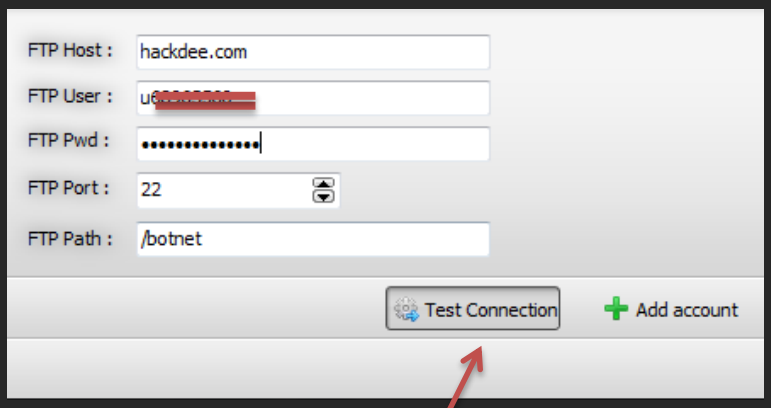
ส่งบันทึกผ่านทาง FTP ลงโฮส

ตัวเลือกนี้เราสามารถใช้ได้ทั้งในโปรแกรม RAT และโปรแกรมคีย์ล็อกเกอร์ทั่วไป แต่ผมจะยกตัวอย่างการใช้งานใน DarkCometRAT ให้ดู แต่ก่อนอื่นเราจำเป็นต้องมีโฮสนะครับ แล้วต้องเป็นโฮสของตัวเอง ผมไม่แนะนำให้ใช้โฮสฟรีนะครับ จากนั้นให้เราสร้าง FTP Account ขึ้นมาในโฮสของเรา.

เปิด DarkComet RAT ขึ้นมาแล้วไปที่ "**Client settings**"

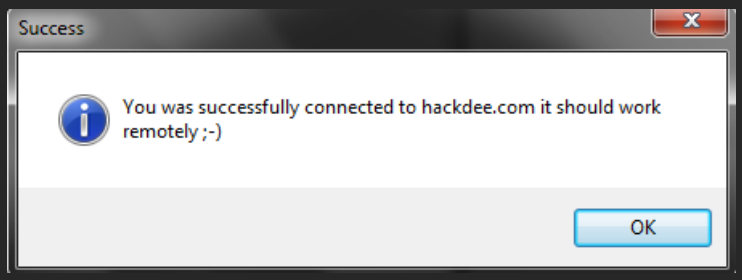


จากนั้นไปที่ **Manager FTP Wallet** ใส่ข้อมูล FTP ของเราลงไป:

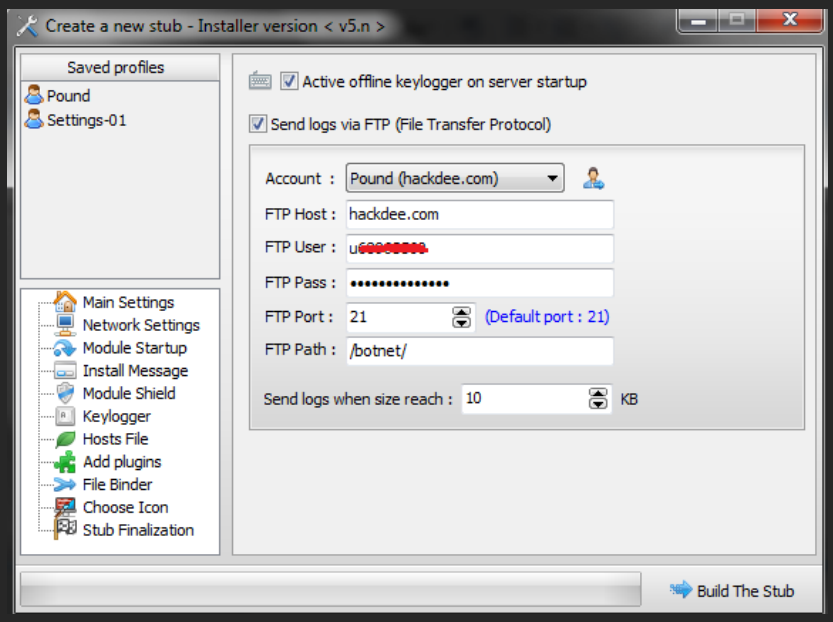


กด **Test Connection** เพื่อทดสอบว่ามันเชื่อมต่อกับ FTP ของเราได้หรือเปล่า

ถ้ามีหน้าต่างเด้งขึ้นมาแบบนี้:



แปลว่า FTP ของคุณทำงาน ให้กด "**Add Account**" ได้เลย.. จากนั้นในขั้นตอนการสร้างโทรจัน ในหน้า "**Keylogger**" ให้เราติกช่อง **Sen logs via FTP** แล้วเลือก Account ที่เรา Save ไว้:



Note: ในช่อง "Send logs when size reach" เราสามารถกำหนดได้ว่าถ้าไฟล์มีขนาดเท่าไหร่ถึงจะให้มันส่งขึ้นไปบนโฮสของเราในแต่ละครั้ง

เท่านี้ล็อกการดักคีย์ทั้งหมดก็จะถูกส่งเข้าไปในโฮสของเราแล้ว วิธีนี้จะช่วยประหยัดเวลาให้คุณไม่ต้องมานั่งเฝ้าหน้าจอเหยื่อตลอด 24 ชม. ^^.

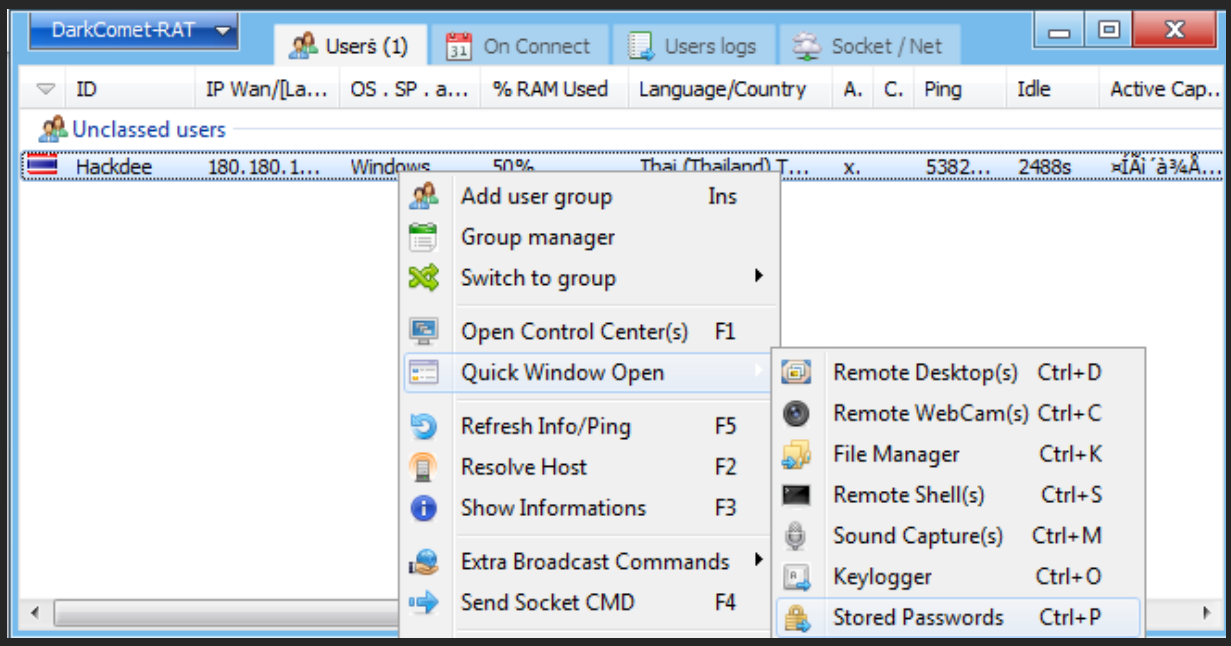
TIP: ใช้ Logs Keylogger เฉพาะเหยื่อที่คุณต้องการ จะได้ไม่กินเนื้อที่โฮส!.

TIP 2: ใช้ FileZilla (ดาวน์โหลดที่ Google) สำหรับการเข้าไปโหลดไฟล์ล็อกในโฮสของเรานะครับ.

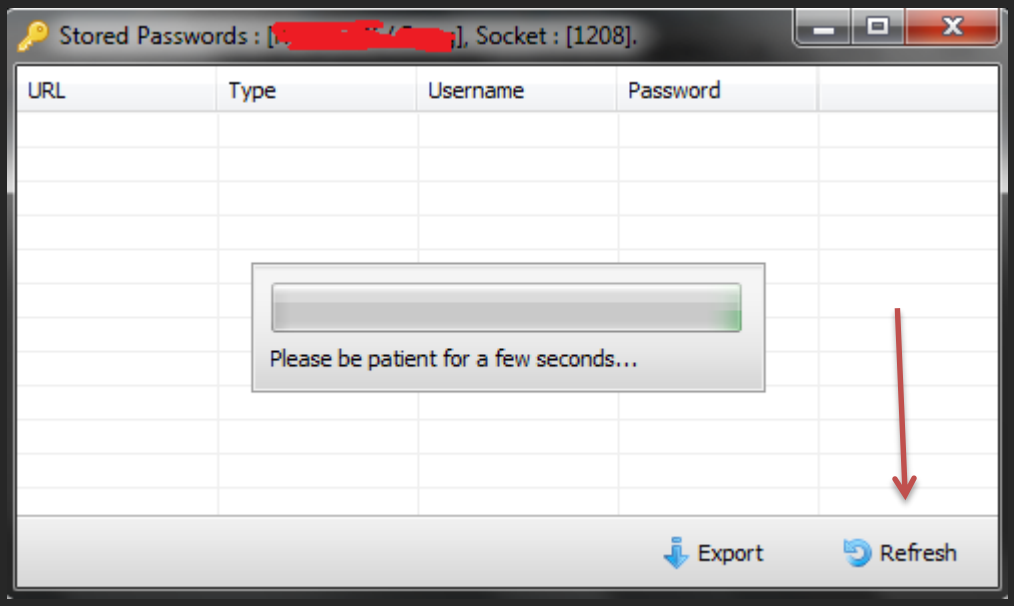
Stealer และวิธีติดตั้ง

Stealer คือโปรแกรม Password Recovery ดีๆนี้เองใช้สำหรับขโมยรหัสผ่านต่างๆ เช่นรหัสผ่านทั้งหมดที่อยู่ใน Chrome, FireFox, Internet Explorer, Msn ฯลฯ ขึ้นอยู่ที่ว่าคนเขียนจะเขียนให้มันขโมยรหัสอะไรได้บ้าง บางตัวสามารถขโมยรหัส Stream และ Filezilla ได้เลย.

ใน DarkComet RAT ก็มีฟังค์ชั่น Stealer นะครับ ให้คลิกขวาที่บอท > **Quick Window Open** > **Stored Passwords**:



กด Refresh แล้วรอสักครู่มันก็จะแสดงรหัสผ่านที่มันขโมยมาได้ทั้งหมดบนหน้าจอ



นอกจากนี้ Stealer ยังมีอีกรูปแบบนึง คือรูปแบบของ Web Based ให้ดูที่ลิงค์นี้ พร้อมวิธีติดตั้งครับ:

http://www.hackdee.net/community/index.php?threads/withuetidtang-stealer.529/

Java Drive-By

Java Drive-By คือโค้ตของจาวาสคริป (JavaScript) เมื่อเรานำโค้ตนี้มาใส่บนหน้าเว็ปไซต์เรา เวลาเปิดหน้าเว็ปไซต์ขึ้นมา ก็จะมีกล่องข้อความจาวาขึ้นมาให้กด Run, เมื่อคุณกด Run มันจะทำการดาวน์โหลดไฟล์ที่ถูกฝังอยู่ในสคริปนั้นแล้วรันอัตโนมัติลงบนเครื่องของคนกดทันที วิธีติดตั้งตามลิงค์ด้านล่างเลยครับ:
http://www.hackdee.net/community/index.php?threads/withuetidtang-java-drive-by.7/

แบบวิดีโอที่ MOD Possible ทำไว้:

http://www.hackdee.net/community/index.php?threads/withuetidtang-java-drive-by-vdo.709/

Note: คุณต้องมีความรู้เกี่ยวกับการอัพโหลดไฟล์ลงเว็ปไซต์ และการตกแต่งหน้า Index.html เล็กน้อย วิธีสมัครเว็ปโฮสฟรีและวิธีอัพโหลดไฟล์ตามลิงค์ด้านล่างเลย:

http://hackdee.net/community/index.php?threads/withuesmakhrewbohsting-laeoiad.929/

Phishing

หลายคนอาจจะเคยได้ยินเกี่ยวกับการแฮกในรูปแบบของการทำ Phishing มาแล้ว หัวข้อนี้ผมจะพาไปเจาะลึก และวิธีการทำ Phishing แบบเต็มรูปแบบซึ่งมีที่นี้ที่เดียวที่สอน เพราะผมลองหาตาม Google ก็เจอเหมือนกัน แต่เขาสอนคร่าวๆ สอนแบบปล่อยให้ งง และไม่ลงลึกถึงใจความสำคัญของการทำ Phishing ดังนั้นห้ามพลาดนะครับ!

Phishing คือการสร้าง "หน้าเข้าสู่ระบบปลอม" "หน้าซื้อของออนไลน์ปลอม" หรือหน้าอะไรก็แล้วแต่เพื่อหลอกให้เป้าหมายกรอกข้อมูลที่เราต้องการ แล้วข้อมูลพวกนั้นก็จะบันทึกอยู่ในล็อกของเรา ศึกษาได้ที่ลิงค์ด้านล่างเลยครับ:

http://www.hackdee.net/community/index.php?threads/bthkhwam-withuetham-phishing-chbabetm.601/

ในบทความนี้คุณจำเป็นต้องมี:

- ความรู้เกี่ยวกับ HTML เล็กน้อย - ปานกลาง
- ความรู้เกี่ยวกับการ สร้างโฮส/จดโดเมน ไปที่ลิงค์นี้ถ้าคุณไม่รู้: http://hackdee.net/community/index.php?threads/withuesmakhrewbohsting-laeoiad.929/
- จินตนาการ **(สำคัญที่สุด)**

ถ้าคุณอ่านบทความจนจบ คุณจะรู้จักวิธีใช้ Phishing ที่ถูกหลัก และ วิธีป้องกันตัวเองจาก Phishing.

ให้ลองนำ SMS Pro มารวมกับการทำ Phishing. โอกาสสำเร็จจะมากขึ้นเป็นเท่าตัว ขึ้นอยู่กับจินตนาการของคุณ:

http://www.hackdee.net/community/index.php?threads/phishing-facebook-karaichchintnakaainkaraehk.1518/

DDoS และ บอทเน็ต

หัวข้อนี้เราจะศึกษาเกี่ยวกับเรื่องของ DDoS และบอทเน็ต. DDoS คือการโจมตีเป้าหมาย มีจุดประสงค์เพื่อให้ระบบของเป้าหมายทำงานผิดปกติ เช่นทำงานช้าลงไปจนถึงขาดการเชื่อมต่อไปเลย. การโจมตีทาง DDoS มักจะโจมตีผ่าน IP Address ของเหยื่อ ลองดูตัวอย่างการโจมตีทาง DDoS กันก่อนครับ:

ยิงเว็ปไซต์:
http://www.youtube.com/watch?v=TZsO51xAFVM

ยิงเซิฟเวอร์:
http://www.youtube.com/watch?v=kuonxBZ6pho

ความแรงของการโจมตีโดย DDoS ก็แตกต่างกันออกไปแล้วแต่อุปกรณ์หรือสคริปที่เราใช้. การยิง DDoS คุณสามารถยิงได้หลายรูปแบบ สามารถยิงได้จาก Windows, Linux หรือในโปรแกรมบอทเน็ต (Botnet Hosting) ทุกอย่างเราจะศึกษากันในหัวข้อนี้ครับ.

การยิง DDoS บน Windows Server โดยใช้ Perl Script

วิธีนี้ผมแนะนำให้ใช้ Windows Server ยิงนะครับ เพราะถ้าเอาเน็ตบ้านเราไปยิงนอกจากเป้าหมายจะไม่เป็นอะไรแล้วเรายังจะขาดการเชื่อมต่อไปสะเอง.

ก่อนอื่นคุณต้องดาวน์โหลดและติดตั้ง Active Perl ลงบนเซิฟเวอร์ของคุณก่อน:

http://www.activestate.com/activeperl/downloads

จากนั้นใช้สคริปนี้ครับ:

http://www.hackdee.net/community/index.php?threads/skhripying-ddos-samhrab-windows-server-perl-script.175/

การยิง DDoS โดยใช้โปรแกรมบอทเน็ต (Botnet Hosting)

โปรแกรมบอทเน็ตคือโปรแกรมสร้างโทรจันครับ แต่เป้าหมายของมันต่างจาก RAT ตรงที่ เหยื่อที่เราแฮกมาได้นั้นเราจะเอามาใช้ในการยิง DDoS แทน ใช่ครับหมายความว่าเราจะใช้คอมฯและเน็ตบ้านของเหยื่อที่เราแฮกมาได้เป็นตัวยิง DDoS! ดังนั้นยิ่งมีบอทที่แฮกมาได้เยอะเท่าไหร่ความแรงของมันก็ยิ่งมากตามไปด้วย.

Warning! ผมแนะนำให้คุณอ่านหัวข้อ "แฮกปลอดภัย" ก่อนที่จะเริ่มใช้วิธีนี้!

วิธีติดตั้งโปรแกรมบอทเน็ตตามลิงค์ด้านล่างเลย คุณสามารถเลือกได้ว่าอยากใช้ตัวไหน โดยส่วนตัวผมแนะนำ **MeTuS** หรือ **IPKiller** นะครับเพราะสมาชิกหลายท่านบอกว่าสองตัวนี้ใช้งานโอเคกว่าตัวอื่น แต่คุณสามารถลองตัวอื่นได้ครับ:

MeTuS Delphi 2.8:
http://www.hackdee.net/community/index.php?threads/1-host-booting-metus-delphi-2-8-phromwithuetidtang.826/

IPKiller 2.0:
http://www.hackdee.net/community/index.php?threads/ddos-ipkiller-v2-0opraekrmbothentaelawithuetidtang.513/

DDoser 4.4:
http://www.hackdee.net/community/index.php?threads/ddoser-4-4-opraekrmbothent-phromwithueaich.187/

Dark DDoser 5.6c:
http://www.hackdee.net/community/index.php?threads/dark-ddoser-v-5-6c-opraekrmbothentaelawithueaich.450/

Tip: ถ้ามีปัญหาเกี่ยวกับการติดตั้ง โพสถามในกระทู้ได้ตลอดครับ.

การยิง DDoS บน Linux

การยิง DDoS บน Linux คือวิธีที่มีประสิทธิภาพมากที่สุดในบรรดาการโจมตีโดย DDoS ทั้งหมดข้างต้น.. การยิงโดยใช้ Linux นั้นมีหลายวิธี ผมจะอธิบายทุกวิธีที่นี้ครับ. ก่อนอื่นผมแนะนำให้ใช้เซิฟเวอร์ **Linux Centos 6.x** (64 Bit) ครับ.

เรามาเริ่มกันที่สคริปยิงพื้นๆบ้านๆกันก่อน:

http://www.hackdee.net/community/index.php?threads/skhripying-ddos-khong-linux.106/

ยิงโดยใช้ลิสไอพี DNS Amplification (Linux):

หรือที่เรารู้จักกันในชื่อ การยิงแบบ UDP Spoofing การยิงแบบนี้เป้าหมายจะไม่สามารถตรวจสอบได้เลยว่าไอพีไหนยิงเข้ามา. ลิสไอพี DNS Amplification คือ ลิสไอพีที่อยู่ในไฟล์ .txt เป็นไฟล์ที่เพิ่มความแรงให้กับการยิง Ddos ของคุณ ไฟล์นี้จะทำงานร่วมกับ DNS Script. ตัวสแกนลิสไอพีมันจะส่งข้อมูลไม่พึงประสงค์เข้าไปในเซิฟเวอร์ที่เราสแกน เพื่อดึงแบนวิทของเซิฟเวอร์นั้นๆมาใช้ในการยิงซึ่งจะทำให้การยิงประเภทนี้แรงกว่าการยิง DDos UDP ธรรมดาแบบปกติถึง 20-40 เท่า! ขึ้นอยู่กับลิสไอพีที่เราสแกน วิธีตั้งค่าและวิธีใช้แบบละเอียดตามลิงค์ด้านล่างเลยครับ:

http://www.hackdee.net/community/index.php?threads/mueaaihm-withuesaeknlisaiophue-dns-amplification-aelawithueaich.773/

WARNING: การยิงแบบ Spoofing IP เซิฟเวอร์ของเราต้องรองรับการทำ Spoof ด้วยนะครับ บางที่มันไม่รองรับ ถ้าไม่รองรับสคริปเราก็ยิงไม่ออก ผมแนะนำที่เหล่านี้:

www.Server4you.net
www.iweb.com
www.ubiquityservers.com
www.serverhub.com
www.servermania.com
www.privatelayer.com

Tip: ใช้เซิฟเวอร์ 100Mbps นะครับ ถ้าใช้ 1000Mbps จะเสี่ยงต่อการโดนถอนถ้าคุณใช้วิธียิงแบบ UDP Spoofing หรือ DNS Amplification.
ของแถม! เนื่องจากว่าผมรักสมาชิกของผมมาก ผมจะแจกสคริปยิงทั้ง Layer 4 และ Layer 7 ให้ฟรีๆ!:
http://www.hackdee.net/community/index.php?threads/aechk-ddos-script-thang-layer-4-aela-7.1686/

IRC Linux Botnet

วิธีนี้คือวิธีที่ผมใช้อยู่ ลองดูตัวอย่างตามวิดีโอด้านล่างนี้:

ยิงเว็ปไซต์:
http://www.youtube.com/watch?v=TZsO51xAFVM

ยิงเซิฟเวอร์:
http://www.youtube.com/watch?v=kuonxBZ6pho

IRC Linux Botnet คือการฝังสคริปโทรจันลงไปบนเซิฟเวอร์ Linux จากนั้นเราจะสามารถควบคุม root ของเซิฟเวอร์ที่รันสคริปโทรจันผ่านทาง IRC! วิธีนี้ใช้ประโยชน์ได้หลายรูปแบบ แล้วแต่จะนำไปใช้ เช่นหากคุณมีเซิฟเวอร์ 10 เครื่อง เวลายิงคุณก็ต้องเข้าไปในเซิฟเวอร์ทั้ง 10 เครื่องเพื่อที่จะยิง แต่ถ้าคุณฝังทั้ง 10 เครื่องไว้ใน IRC คุณก็แค่เข้าไปใน mIRC แล้วสั่งยิงจากที่นั้นพร้อมกันทีเดียว 10 เครื่อง! นอกจากจะสะดวกสบายแล้วยังเพิ่มความแรงให้การยิงของคุณเป็นเท่าตัว.

ก่อนอื่นคุณจำเป็นต้องติดตั้ง Unreal IRCD บนเซิฟเวอร์ของคุณเองก่อน:
http://www.hackdee.net/community/index.php?threads/withuetidtang-unreal-ircd-ain-linux-centos.249/

จากนั้นดาวน์โหลด mIRC ไว้ในเครื่องคอมฯของคุณเอง ดาวน์โหลดที่นี้:
http://www.mirc.co.uk/get.html

วิธีติดตั้ง IRC Linux Bot และคำสั่งต่างๆ:
http://www.hackdee.net/community/index.php?threads/withuetham-linux-irc-botnet.353/

Note: วิธีเข้าไปสร้างห้อง IRC ก็ไม่ยากครับ ใครไม่เคยใช้อาจจะ งง หน่อยแต่ก็ไม่ยากลองค้นหาใน Google หรือลองด้วยตัวเองดูก่อนถ้าไม่ได้จริงๆ ให้โพสถามในบอร์ด ผมไม่ขอลงในหนังสือนะครับ เพราะมันจะกินเนื้อที่โดยใช่เหตุ.

Web Booter (Stresser)

โอเคครับ ถึงตรงนี้คุณคงรู้จักวิธียิงรูปแบบต่างๆแล้ว นี่คือหัวข้อสุดท้ายของ DDoS ที่ผมจะสอน ก่อนอื่นดูวิดีโอนี่ก่อน คุณจะได้มีไอเดียว่าอะไรคือ Web Booter:

http://www.youtube.com/watch?v=4Chr6D_zcI4

ใช่ครับ Web Booter คือการยิง DDoS โดยออกคำสั่งผ่านหน้าเว็ปไซต์ หลักการของมันคือการใช่ API เป็นตัวเชื่อมในการส่งคำสั่งยิงที่ถูกสั่งบนหน้าเว็ป ส่งต่อไปบนเซิฟเวอร์ Linux ที่มีสคริปยิงอีกที (เดียวจะอธิบายเพิ่มเกี่ยวกับ API ในกระทู้). ข้อดีของการใช้ Web Booter คือเราสามารถให้คนอื่นเข้าสู่ระบบไปใช้บริการ DDoS ของเราบน Web Booter ได้อยู่ในขอบเขตที่เรากำหนด.

วิธีติดตั้ง **Web Booter** แบบละเอียดพร้อม Source โดยคุณ **kshooter** :
http://www.hackdee.net/community/index.php?threads/skhripewbbutetor-phromwithuetham.1013/

วิธีสร้าง **API** สำหรับ Web Booter โดยคุณ **kshooter** :
http://www.hackdee.net/community/index.php?threads/withuesrang-api-ainluenuks.306/

เราสามารถสร้าง **API** เพื่อส่งคำสั่งยิงไปยังห้อง IRC ที่มี Linux Botnet ของเรา ได้อีกด้วย! ตามลิงค์ด้านล่างเลยครับ:
http://www.hackdee.net/community/index.php?threads/withuetidtang-api-samhrab-irc-linux-botnet.501/

คุณสามารถใช้ Source ของ Web Booter ตัวอื่นจาก Google ก็ได้นะครับ วิธีการติดตั้งก็คล้ายๆกัน.

Note: โฮสบางโฮสจะบล็อกฟังค์ชั่น SQL บางตัวของ Web Booter เช่นบางโฮสบล็อกคำสั่งนับเวลายิงถอยหลัง บางโฮสบล็อกคำสั่งการเข้าสู่ระบบ ดังนั้นสิ่งที่ยากที่สุดในการทำ Web Booter คือการหาโฮสที่ไม่บล็อกฟังค์ชั่น SQL ใน Source ของเราเลย แต่ถ้าคุณมีความรู้ด้าน PHP และ SQL คุณสามารถแก้ไขดัดแปลงฟังค์ชั่นต่างๆ ให้เข้ากับโฮสนั่นๆได้.

WEBSITE HACKING

SQL Injection

SQL Injection คือการแฮกเว็ปไซต์ต่างๆผ่านทางช่องโหว่ของ SQL หัวข้อนี้ผมจะรวมทุกบทความเกี่ยวกับการแฮกเว็ปไซต์โดย SQLi และวิธี Bypass WAF ต่างๆ. ก่อนอื่นผมแนะนำให้เริ่มจากการทำ SQLi แบบพื้นฐาน (Union Based) ก่อนนะครับ ไปตามลิงค์ด้านล่าง:

Union Based – มือใหม่เริ่มที่นี้เลย (มีวิดีโอประกอบ):
http://hackdee.net/community/index.php?threads/sqli-aehkewpaistody-sqli-mueaaihmerimthuenuekhrab-union-based.100/

วิธี Bypass หน้าแอดมินของเว็ปไซต์ที่มีช่องโหว่ SQL (มีวิดีโอประกอบ):
http://hackdee.net/community/index.php?threads/sqli-khamsang-bypass-hnalokoin-admin.125/

จากนั้นคุณสามารถเริ่มศึกษาเกี่ยวกับรูปแบบอื่นๆของการทำ SQLi ต่อ:

Blind Injection (Boolean Based):
http://hackdee.net/community/index.php?threads/sqli-kartham-blind-injection-boolean-based-injection.345/

Error Based Injection:
http://hackdee.net/community/index.php?threads/sqli-kartham-error-based-injection.362/

Double Query Based Injection:
http://hackdee.net/community/index.php?threads/sqli-kartham-double-query-injection.379/

ทั้งหมดนี้คือ "**พื้นฐาน**" ของการแฮกเว็ปไซต์โดย SQL Injection!.

ถาม: ทำไมการทำ SQLi ถึงมีหลายรูปแบบ?
ตอบ: เพราะบางทีการทำ SQLi แบบ Union Based ก็ไม่ทำงานเสมอไป และบางเว็บไซต์คุณอาจจะต้องใช้เทคนิคการ Bypass ที่ผมจะสอนในหัวข้อต่อไป.
Tip: คุณสามารถทดลองแฮกเว็บไซต์ที่มีช่องโหว่ของ SQL ที่ผมนำมาแจกได้ที่:
http://hackdee.net/community/index.php?threads/lisewbaistthuemuechongohw.1853/

Bypassing WAF

WAF ย่อมาจาก Web Application Firewall ที่ทำหน้าที่เป็นตัวกรองคำสั่งแปลกปลอมต่างๆที่เชื่อมต่อกับเว็ปไซต์นั่น เช่น คำสั่งของ SQLi และ XSS. WAF แต่ละตัวไม่เหมือนกัน รูปแบบการกรองคำสั่งของมันก็ต่างกันออกไป เช่น WAF บางตัวกรองคำว่า Union Select บางตัวกรองคำสัญลักษณ์ต่างๆเช่นคอมม่า บางตัวกรอกอักษรตัวใหญ่ตัวเล็ก เป็นต้น.

หัวข้อนี้เราจะมาศึกษาเกี่ยวกับวิธีการ Bypass WAF ในรูปแบบต่างๆและตัวอย่างการทำ Bypass WAF ก่อนอื่นมาดูตัวอย่างการทำ Bypass WAF บางส่วนกันก่อน:

การ Bypass WAF ที่บล็อกคอมม่า:
http://hackdee.net/community/index.php?threads/sqli-thamyangaingtha-khomma-thukblokody-waf.308/

การ Bypass Error 1242:
http://hackdee.net/community/index.php?threads/sqli-withue-bypass-error-1242-odyaich-substr-function.473/

การ Bypass ค่าจำกัดของ Group_Concat:
http://hackdee.net/community/index.php?threads/sqli-bypass-khachamkadkhong-group_concat.322/

การ Bypass Error 404:
http://hackdee.net/community/index.php?threads/sqli-bypass-waf-duai-comments.1028/

การ Bypass Error 400 (เว็บกระทรวง ICT):
http://hackdee.net/community/index.php?threads/sqli-bypass-error-400-bad-request.1076/

ข้างต้นเป็นแค่ตัวอย่างเท่านั้นถ้าต้องการศึกษาการ Bypass แบบเต็มให้ไปที่นี้:
http://hackdee.net/community/index.php?threads/sqli-bypassing-waf-s.304/

Shells & Defacing

หลังจากที่คุณแฮกเข้าไปในหน้าแอดมินของเว็บไซต์ได้แล้ว คุณสามารถฝั่ง Shell เข้าไปเพื่อควบคุมเว็บไซต์นั้นๆ เราสามารถลบไฟล์ เปลี่ยนไฟล์ หรือ Deface หน้าเว็บไซต์ที่เราแฮกมาได้อย่างอิสระ (อาจสงสัยว่าอะไรคือ Deface การ Deface คือการเปลี่ยนหน้าเว็บไซต์ให้เป็นหน้าเว็บที่เราสร้างขึ้นเอง เพื่อให้คนอื่นหรือเจ้าของเว็บนั้นๆรู้ตัวว่าโดนแฮก) วิธีการฝั่ง Shell และสคริป Shell ไปที่นี้เลย:

http://hackdee.net/community/index.php?threads/oaphohld-shell-eplueynhnaewpaisd.223/

แต่กับบางเว็บไซต์คุณก็จำเป็นต้อง Bypass เพื่อที่จะอัพ Shell ลงไปได้:

http://hackdee.net/community/index.php?threads/upload-shell-ody-tamper-data.1262/

แค่นี้คุณก็รู้ถึงวิธีฝัง Shell และการ Deface หน้าเว็บไซต์ต่างๆ แต่ถ้าคุณมือใหม่ด้าน **HTML** และไม่รู้จะสร้างหน้า Deface ของตัวเองยังไง ผมแนะนำให้เรียนพื้นฐานเกี่ยวกับ HTML ได้ที่นี้:

http://hackdee.net/community/index.php?forums/erian-html.61/

แฮกเว็บไซต์โดย XSS (Cross Site Scripting)

ทำความรู้จักกับ XSS วิธีทำและวิธี Bypass:
http://hackdee.net/community/index.php?threads/aehkewpaistody-xss-cross-site-scripting.284/

วิธี Bypass Filter แบบลึกอีกมากมาย:
http://hackdee.net/community/index.php?threads/xss-khamsang-bypass-xss-makmai-xss.1091/

วิธี Deface หน้าเว็บไซต์ (โดยแอดมิน Possible):
http://hackdee.net/community/index.php?threads/xss-withueeplueynhnataewpaistedngmahnaewbera-vdo-hd.563/

Pentesting With Kali Linux

คอยติดตามบอร์ดนี้เพื่อศึกษาเกี่ยวกับการทำ Pentesting บน Kali Linux:

http://hackdee.net/community/index.php?forums/pentesting.69/

แฮกปลอดภัย

สิ่งที่สำคัญที่สุดในการเป็นแฮกเกอร์คือ คุณต้องมั่นใจว่าคุณแฮกแล้วคุณจะ "ปลอดภัย". หัวข้อนี้เราจะมารู้จักวิธีแฮกแบบปลอดภัย และวิธีป้องกันตัวเองจากแฮกเกอร์.

การแฮกโดยการใช้ RAT (โทรจัน)

ใช้ VPN เพื่อซ่อนไอพีจริงของคุณ เพราะถ้าคุณใช้ไอพีจริงๆของคุณทำการแฮกเป็นสิ่งที่อันตรายมากๆ เพราะเหยื่อสามารถเช็คไอพีที่เชื่อมต่อเข้ามาในคอมฯของเขาได้อย่างง่ายดาย โดยใช้คำสั่ง Netstat ใน CMD และคุณจะโดนตำรวจมาเคาะประตูบ้านภายใน 24 ชั่วโมงแน่นอน. VPN ที่สามารถเปิดพอทและใช้งานกับ RAT ได้คือ nVPN. สามารถสั่งซื้อได้ที่นี้:

http://hackdee.net/community/index.php?threads/nvpn-vpn-epidphotaid.490/

วิธีติดตั้ง nVPN:

http://hackdee.net/community/index.php?threads/nvpn-withuetidtang-nvpn.109/

วิธีเปิดพอทใน nVPN:

http://hackdee.net/community/index.php?threads/nvpn-withueepidphotain-nvpn-port-forwarding.110/

นอกจากนั้น สิ่งที่สำคัญมากๆอีกอย่างคือ อย่าเที่ยวไปบอกคนอื่นเขาว่าคุณแฮกคนนั้น แฮกคนนี้ได้ เพราะนั้นเป็นสิ่งต้องห้ามที่แฮกเกอร์ทุกคนไม่ควรทำเด็ดขาด! ถึงแม้ว่าคุณจะปลอดภัยจากกฎหมาย เพราะคุณทำลายหลักฐานได้ทั้งหมด แต่คุณก็จะเพิ่มช่องโหว่ให้ตัวเอง นั้นคือการที่คนอื่นรู้ถึงการมีตัวตนของคุณ! ดังนั้น หักห้ามใจ อย่าบอกคนที่เราไม่ไว้ใจว่าเราไปทำอะไรมาบ้าง.

แฮกเว็บไซต์

แนะนำให้อ่านหัวข้อ "การป้องกันกันตัวเองรูปแบบออนไลน์โหมด" ในกระทู้:
http://hackdee.net/community/index.php?threads/tut-aehkplodphai.1271/

การป้องกันตัวเองจาก Hacker

คุณจะป้องกันตัวเองได้จากแฮกเกอร์ได้แบบเต็มรูปแบบก็ต่อเมื่อคุณรู้จักวิธีการแฮกในรูปแบบต่างๆเป็นอย่างดี ซึ่งทุกอย่างคุณสามารถศึกษาได้ใน E-Book เล่มนี้ทั้งหมด.

ที่ๆดีที่สุดที่คุณจะเริ่มศึกษาเกี่ยวกับวิธีการป้องกันตัวเองได้ดีที่สุดคือ:
http://hackdee.net/community/index.php?threads/secure-your-ass-pongkantuakhunchakothrchan.680/

และหัวข้อ "การป้องกันแบบออฟไลน์โหมด" ในกระทู้:
http://hackdee.net/community/index.php?threads/tut-aehkplodphai.1271/

และที่สำคัญที่สุดคุณต้องไม่ "ขี้เกียจ"... หลายคนรู้ว่าควรทำอย่างไร แต่ความด้วยความขี้เกียจ ทำให้เกิดความประมาท และนั่นจะทำให้เกิดช่องโหว่ขนาดใหญ่. ดังนั้น การเสียเวลาเล็กๆน้อยๆ ป้องกันตัวเองไว้ก่อน มันคุ้มกว่าต้องมานั่งแก้ทีหลัง.

Facebook Hacking 2014

ของแถมท้ายเล่ม บทความสอนแฮกเฟสบุคที่ได้ผลจริง 100 % ฉบับ 2014:
http://hackdee.net/community/index.php?threads/facebook-hacking-2014-withuekaraehk-facebook-bthkhwamkhunphaphaidphlchring-100.1774/

To be continue....