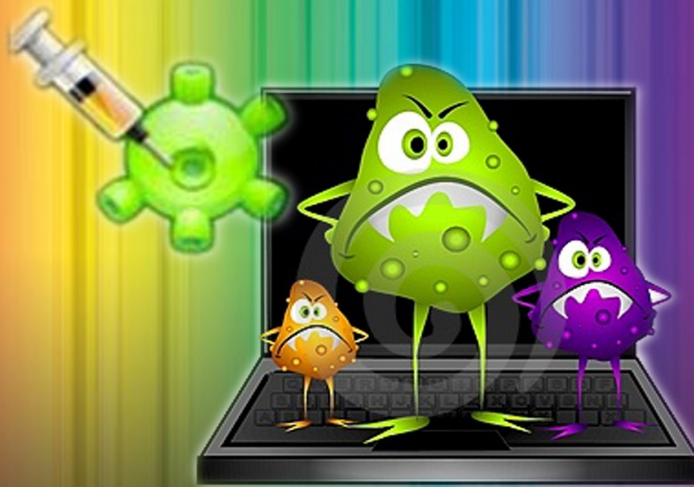


# VIRUS Fla hy (Win32)




237211-2554 COMPUTER NETWORKING FOR EDUCATION



## คำนำ

หนังสือเล่มนี้เป็นส่วนหนึ่งของวิชาเครือข่ายคอมพิวเตอร์เพื่อการศึกษา 237211 เป็นเรื่องเกี่ยวกับไวรัส Flashy จัดทำขึ้นเพื่อให้ความรู้และวิธีการกำจัดไวรัส Flashy ซึ่งคณะผู้จัดทำตั้งใจจัดทำขึ้นอย่างเต็มที่ เพื่อเป็นประโยชน์แก่ผู้ที่ต้องการศึกษา และผู้อ่านทั่วไป แต่ถ้ามีความผิดพลาดประการใด คณะผู้จัดทำขออภัย ณ ที่นี้ด้วย



## สารบัญ

เรื่อง	หน้า
อาการที่พบ	1
วิธีแก้ปัญหา	2
โปรแกรมที่ใช้สแกนไวรัส Flashy	11
บรรณานุกรม	13



# ไวรัส Flashy

(Win32/Disabler.I trojan)

## อาการที่พบ

1. ไม่สามารถเรียกใช้ **Task Manager, Registry Editor** และ **Folder Option** ได้ ไม่ว่าจะเรียกด้วยวิธีใด
2. อยู่ดีๆ เครื่องก็ตั้ง **password admin** ให้ทุกอย่างที่เราไม่เคยตั้งทำให้เราเข้าเครื่องตัวเองไม่ได้แต่พอลองใส่รหัสผ่านว่า **hacked** เข้าได้
3. เมื่อมีการเสียบ **Flash Drive** หรือ **Memory Card** เข้าไปใน Card Reader แล้วหากว่าใน Memory Card นั้นมี Folder อยู่ Folder เหล่านั้นจะถูกเปลี่ยนให้ไปอยู่ในสถานะ Hidden ทำให้เราไม่สามารถมองเห็น Folder เหล่านั้นได้

---

---

## วิธีแก้ปัญหา

**\*\* ขั้นตอนต่างๆต้องทำใน Safe mode ถึงจะได้ผล**

**เข้า Safe Mode ด้วยการกด F8 รั้วๆตอน boot เครื่อง**

### ขั้นตอนที่ 1

ถ้าเครื่องที่มีอาการหนักจะถูกตั้งรหัสผ่าน Administrator เอาไว้ ให้ทำการแก้ไขโดยพิมพ์คำว่า hacked เป็นรหัสผ่าน ซึ่งหากไม่รู้วิธีแก้ปัญหาโดยการติดตั้ง Windows ใหม่อย่างเดียว

### ขั้นตอนที่ 2

เมื่อเราเข้าวินโดวได้แล้วให้เราหยุดการทำงานของมันก่อนโดยกด **Ctrl+Alt+Delete** จะเข้าสู่ Windows task Manager แล้วเลือกคลิก Flashy.exe แล้วคลิก End Process ตรงมุมขวาด้านล่าง

---

---

---

---

### ขั้นตอนที่ 3

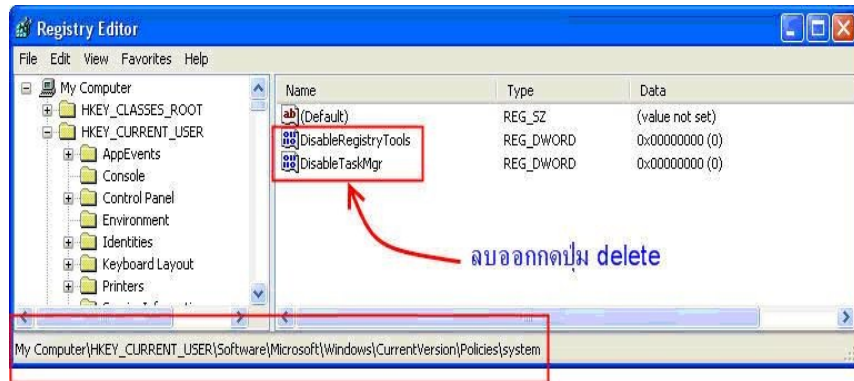
กรณีถ้าเข้า Windows Task Manager ไม่ได้(ถ้าเข้าได้ให้ข้ามไปขั้นตอนที่ 6) ให้เราเข้าไปแก้ไขใน registry แต่ไวรัสยังปิดการเข้าใช้งาน Registry เอาไว้อีกให้ใช้ตัว Unhookexec.inf ปลดล็อคก่อนโดยดาวน์โหลด เมื่อโหลดมาแล้วแตกไฟล์ แล้วก็คลิกขวาที่ไฟล์ UnHookExec.inf แล้วเลือก Install แต่ถ้าเครื่องไหนที่ติดไวรัสหน้าจอภาษาจีนด้วย ต้องฆ่าก่อนไม่อย่างนั้นจะใช้ UnHookExec.inf ไม่ได้ผล

### ขั้นตอนที่ 4

จากนั้นก็เข้าใช้งานส่วน Registry ได้ครับ เมื่อเข้าได้แล้วก็ไปทำการแก้ไข Registry ให้เครื่องใช้งาน Task Manager ได้ครับ โดยไปที่ Start > Run พิมพ์ regedit กด OK แล้วเข้าไปลบคีย์ตามนี้ HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\system

---

---



แล้วก็ลบ DisableRegistryTools และ DisableTaskMgr ออก

### ขั้นตอนที่ 5

เมื่อลบออกได้แล้วก็ไปทำตาม ข้อ 2

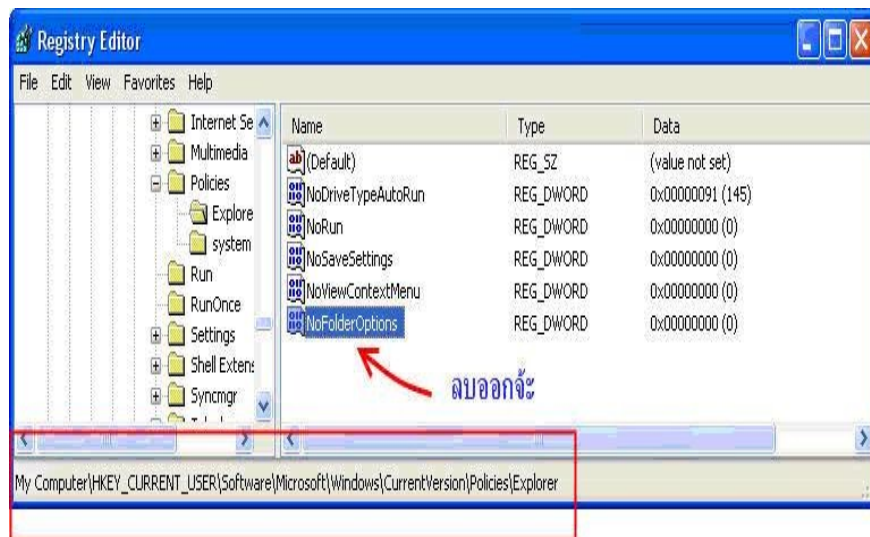


## ขั้นตอนที่ 6

แล้วตอนนี้มันก็หยุดการทำงานแล้วครับ ต่อไปเราต้องเข้า regedit แล้ว ไปที่ Start > Run พิมพ์ regedit แล้วเข้าไปลบคีย์ตามนี้

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\

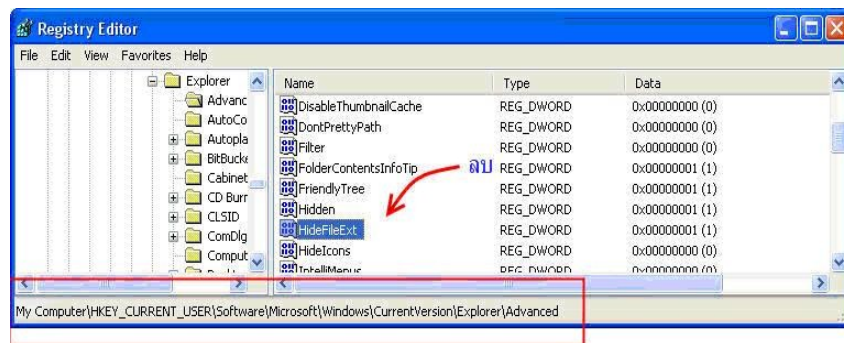
ลบ NoFolderOptions





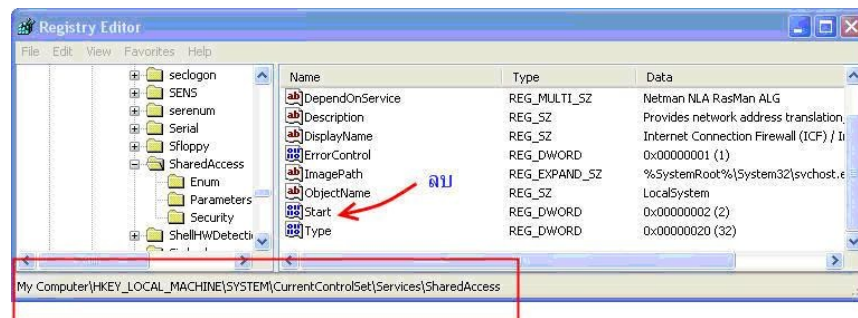
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\

លឿន HideFileExt



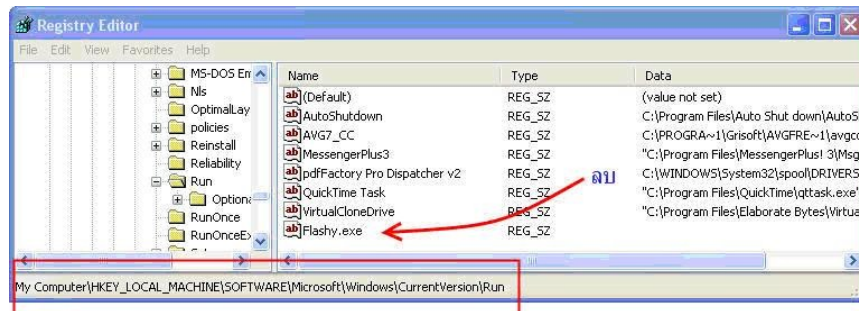
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\

លឿន Start



HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows  
\CurrentVersion\Run\

ลบ Flashy.exe



จากนั้นคลิก Start\Programs\Startup\ ลบ SystemID.pif  
จากนั้นคลิก Start > Run พิมพ์ msconfig ไปที่  
แถบ startup ยกเลิกติ๊กถูกหน้า systemID  
รีสตาร์ทเครื่องใหม่แล้วลองกด Ctrl+Alt+Delete ดู  
ว่า Flashy.exe ยังมีการทำงานอีกหรือไม่ ถ้าไม่มีแสดง  
ว่าเรียบร้อยแล้ว

---

---

## การแก้ไขส่วนที่ไวรัสสร้าง ให้เราต้องใส่รหัส ทุกครั้ง เวลาจะเปิดเครื่อง

### ขั้นตอนที่ 1

คลิก Start > Setting > Control panel > User accounts เลือก User แรก (Administrator) จะสังเกตเห็นว่ามีข้อความแสดงว่า Password protected มีการใช้รหัสผ่านป้องกันอยู่ให้คลิกที่ User แรก (Administrator)

### ขั้นตอนที่ 2

เลือกหัวข้อ Change a password พิมพ์รหัสผ่าน Hacked ในช่องแรก (ช่องรหัสผ่านเดิม) ช่องที่เหลือเว้นว่างไว้ ยืนยันการเปลี่ยนรหัสผ่าน แล้วลองรีสตาร์ทเครื่องใหม่ หรือ Start > Run พิมพ์ regedit > คลิก OK แล้วไปตามนี้ [HKEY\\_LOCAL\\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon](HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon)

---

---

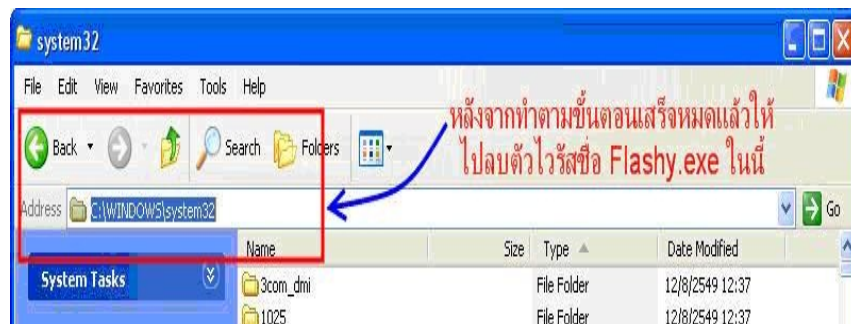
แก้สตริงคีย์ตามนี้ครับหากไม่มีก็คลิกขวาเลือก New > String value ตามนี้

"AutoAdminLogon"="1"

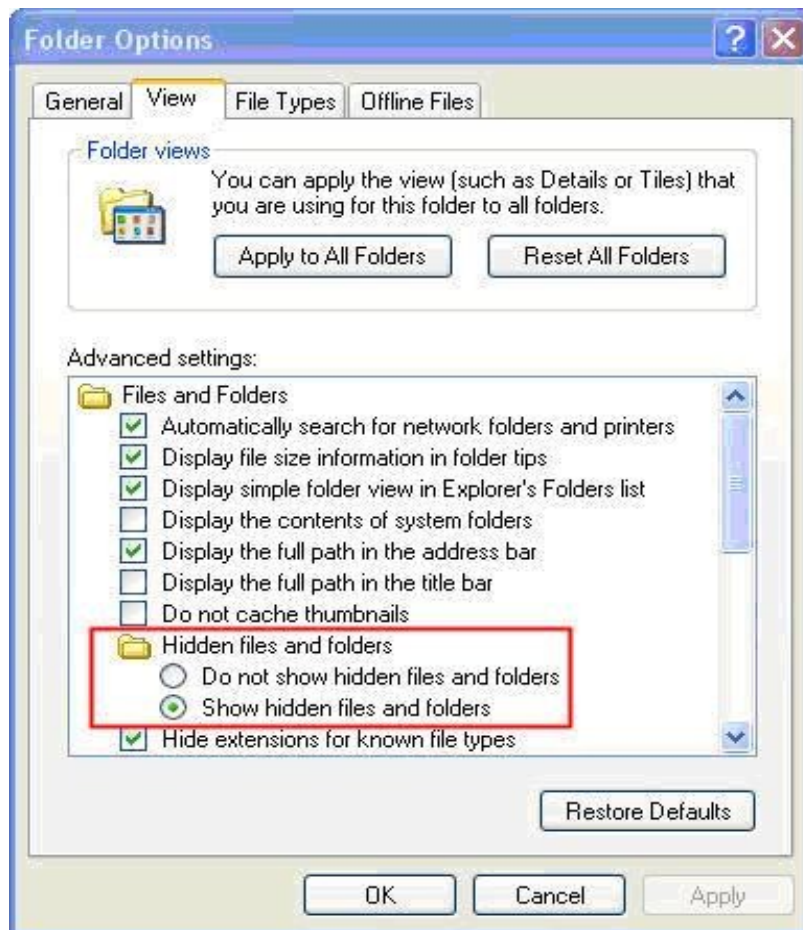
"DefaultUserName"=" ชื่อผู้ใช้"

"DefaultPassword"="hacked"

**\*\* หลังจากทำตามขั้นตอนเสร็จหมดแล้วให้ไปลบตัวไวรัสชื่อ Flashy.exe ใน C:\WINDOWS\system32**



\*\* ต้องเปิด Show hidden File ก่อนถึงจะเห็น วิธีการ  
เปิด Show hidden File  
ทำได้โดย Tools > Folder Option > Show hidden files and  
folders > คลิก ok

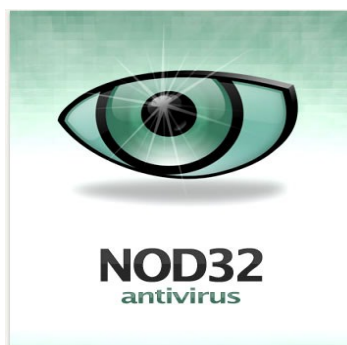
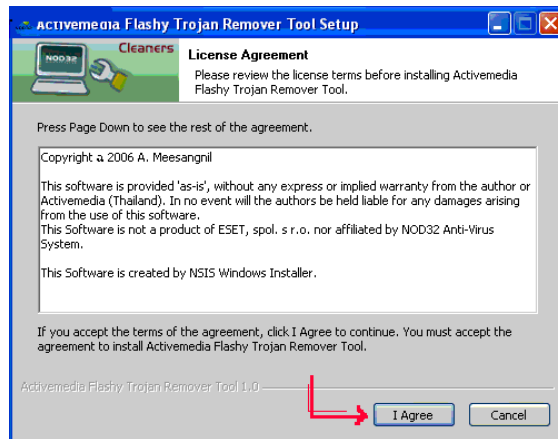


---

---

## โปรแกรมที่ใช้สแกนไวรัส Flashy (Win32/Disabler.I trojan)

😊 โปรแกรม NOD32 MyGril-Fix



---

---

😊 โปรแกรม Trojan



😊 โปรแกรม BitDefender 9





  


## อ้างอิง

<http://intranet.gs.kku.ac.th/km/index.php?option=show&id=4> สืบค้นข้อมูลเมื่อ 23/09/54

<http://antivirus.nabia10.com/virus-t/girl.html>

สืบค้นข้อมูลเมื่อ 20/09/54





## สมาชิกในกลุ่ม

- 1.นางสาวศิริวิภา กุมปรุ 533050201-9
  - 2.นางสาวธิตาทิพย์ กุมนัน 533050197-4
  - 3.นางสาวจันทรา ที่อุปมา 533050184-3
  - 4.นางสาวจิตภา ศิริพรรณ 533050335-8
  - 5.นายพิทักษ์ สมบรรณ 533050343-9
- คณะศึกษาศาสตร์ สาขาคอมพิวเตอร์ศึกษา  
มหาวิทยาลัยขอนแก่น